NETLOCK
Bizalmi Szolgáltatási Rend
Minősített Időbélyeg-szolgáltatásra

NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság

A dokumentum magyar neve:	NETLOCK Bizalmi Szolgáltatási Rend Minősített Időbélyeg-szolgáltatásra
A dokumentum angol neve:	NETLOCK Qualified Trust Service Policy for Timestamp Service
Verzió:	20170615
Azonosító szám (OID):	1.3.6.1.4.1.3555.1.16.20170615
Jóváhagyás időpontja:	2017.06.15.
Hatály kezdőnapja:	2017.06.19.
Oldalak száma:	a fedlappal együtt 61 oldal
Készítette	**Szabó Zoltán** PKI termékmenedzser **Varga Viktor** Chief Architect
Jóváhagyta	**dr. Fehér Zsófia**, Jogtanácsos

© COPYRIGHT, NETLOCK KFT. - MINDEN JOG FENNTARTVA

Tartalom

1 Bevezetés

Jelen dokumentum a NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság (továbbiakban: Szolgáltató) szabálygyűjteménye, melynek célja, hogy összefoglalja és rendszerezze azokat a minimum követelményeket és feltételeket, amelyek a Szolgáltató minősített bizalmi időbélyeg-szolgáltatásának nyújtására és igénybevételére vonatkoznak (a továbbiakban: Szolgáltatási Rend).
A dokumentumban alkalmazott fogalmakat és rövidítéseket illetően lásd az 1.6 fejezetet.

1.1 Áttekintés

1.1.1. Szabványok és előírások

Jelen dokumentum Szolgáltató bizalmi minősített időbélyeg-szolgáltatására vonatkozó elvárásokat tartalmazza:
A dokumentum az RFC 3647 szabvány szerinti szerkezetet követve készült. A dokumentum az eIDAS, az Eüt. (lásd 1.6.2 Rövidítések) és egyéb releváns hazai jogszabályok, valamint az ETSI EN 319401, az ETSI EN 319421 és az ETSI EN 319422 szabványok elvárásait foglalja össze. Az egyes fejezetcímek csak a tartalom adott logikai rend szerinti rendezésére szolgálnak, a rendelkezések értelmezése tekintetében nem irányadók.
Az elvárásoknak való megfelelést a NetLock Minősített Bizalmi Szolgáltatási Szabályzat Időbélyeg-szolgáltatásra dokumentum ismerteti.

1.1.2 A Szolgáltató adatai

Név:	NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság
Rövidített név:	NETLOCK Kft.
Székhely:	1101 Budapest, Expo tér 5-7.
Postázási cím:	1439 Budapest, Pf. 663
Cégjegyzékszám:	01-09-563961
Adószám:	12201521-2-42
Telefonszám:	(1) 437-6655
Fax:	(1) 700-2828
Weboldal:	www.netlock.hu
Kikötések és feltételek közzététele:	www.netlock.hu/html/dok.html
Ügyfélkapcsolati e-mail:	info@netlock.hu
Megrendelések, dokumentummásolatok, szerződések küldése:	igenylesek@netlock.hu
NETLOCK Szabályzatelfogadó Egység email címe:	szee@netlock.hu

Ügyfélfogadás / Nyitvatartás	A Szolgáltató weboldalán feltüntetett helyen és időintervallumban

Az Eat.[1] rendelkezéseinek megfelelő minősített szolgáltatóként a Bizalmi Felügyelet 2003. március 19-én vette nyilvántartásba a Szolgáltatót. Regisztrációs szám: MH-1372-12/2003.

Az Eat. rendelkezéseinek megfelelő minősített archiválás szolgáltatóként a Bizalmi Felügyelet 2010. szeptember 15-én vette nyilvántartásba Szolgáltatót. Regisztrációs szám: HL/18188-4/2010.

A Bizalmi Felügyelet Eat szerinti szolgáltatásokat tartalmazó nyilvántartásának elérhetősége: http://webpub-ext.nmhh.hu/esign/

Jelen Szolgáltatási Rend az eIDAS rendelkezéseinek megfelelő minősített bizalmi tanúsítványszolgáltatás nyújtásával kapcsolatos követelményeket tartalmaz. Szolgáltató e szolgáltatások nyújtását kizárólag a Szolgáltatási Szabályzatban megadott vonatkozó jogszabályi feltételek – például megfelelőségértékelés, Szolgáltató és szolgáltatása bizalmi listán történő feltüntetése és felügyeleti nyilvántartásba vétel – teljesülése esetén kezdheti meg.
A Bizalmi Felügyelet eIDAS szerinti minősített szolgáltatókat és szolgáltatásokat tartalmazó közhiteles nyilvántartásának elérhetősége:

http://webpub-ext.nmhh.hu/esign2016/szolgParams/init.do?tipus=mi

Szolgáltató bizalmi felügyeleti nyilvántartási száma: EF/15066-3/2017

Az EU bizalmi lista (EUTSL) elérhetőségei:

- géppel feldolgozható (xml) formátumban: http://nmhh.hu/tl/pub/HU_TL.xml
- olvasható (pdf) formátumban: http://nmhh.hu/tl/pub/HU_TL.pdf

Szolgáltató jogosult az EU Trust Mark[2] használatára a minősített szolgáltatásai tekintetében.

1.2 A dokumentum neve és azonosítás

A dokumentum nevét és OID azonosítóját lásd a fedlapon (első számozás nélküli oldal a Szolgáltató logójával) - "A dokumentum magyar neve" és "A dokumentum angol neve" valamint az "Azonosító szám (OID)" sorokban.

A dokumentum többi oldalain a dokumentum magyar neve a láblécben, OID azonosítója pedig a fejlécben kerül feltüntetésre.

Jelen dokumentum egyike a Szolgáltató által kiadott azon dokumentumoknak, amelyek az általa nyújtott szolgáltatások feltételeit együttesen szabályozzák. Ilyen dokumentumok továbbá például az Általános szerződési feltételek, a Szolgáltatási szerződés, a szolgáltatási szabályzatok, az Ügyfelekkel és a Partnerekkel kötött egyéb szerződések.

A jelen dokumentumban Szolgáltatónak nevezett entitás a NETLOCK Kft. - adatait lásd az 1.1.2 pontban.

[1] Az elektronikus aláírásról szóló 2001. XXXV. törvény – már nem hatályos
[2] https://ec.europa.eu/digital-single-market/en/eu-trust-mark

1.2.1 Szolgáltatásazonosító

A Szolgáltatónak az időbélyeg-válaszban szabványos azonosítót vagy maga által képzett és nyilvántartott azonosítót fel kell tüntetnie, hogy azonosítsa az időbélyegzésre vonatkozó szabványos vagy egyedi hitelesítési szabályokat és kinyilvánítsa az azoknak való megfelelését.
A Szolgáltató által alkalmazott azonosítók az alábbiak:

Azonosító	**Hitelesítési Rend (vagy Szolgáltatási gyakorlat) neve**	**OID**
BTSP	Best practices policy for time-stamp Legjobb időbélyegzési gyakorlat (**minősített időbélyegzők számára)** (A fenti szabványos OID helyett szerepelhet Netlock OID is az időbélyegzés során is, melynek jelentése ugyanez.)	0.4.0.2023.1.1

1.2.2 Dokumentum revíziók

OID	Hatály	Változás leírása	Készítő
-	nem hatályosított verzió	Egységes – eIDAS szerinti minősített és nem-minősített tanúsítvány-, időbélyeg- és archiválásszolgáltatásokat egyaránt tartalmazó – szolgáltatási rend első nem nyilvános tervezete. Jelen tervezet hatálybalépéséig Szolgáltató minősített időbélyeg-szolgáltatását a 2008. január 9-én hatályba lépett, 1.3.6.1.4.1.3555.1.16.20080107 verziójú Általános időbélyegzési rend szabályozza.	Almási János dr. Barabás Anett Varga Viktor Szabó Zoltán
1.3.6.1.4.1.3555.1.16.20170427	nem hatályosított verzió	Az első nem nyilvános tervezetverzióból a minősített és nem-minősített tanúsítvány- valamint minősített archiválásszolgáltatásra vonatkozó előírások törlésével készített, kizárólag az eIDAS szerinti minősített időbélyeg-szolgáltatásra vonatkozó követelményeket tartalmazó új verziójú nem nyilvános tervezet a minősített időbélyeg-szolgáltatásra vonatkozó követelmények pontosításával. Ezzel párhuzamosan külön verziók készültek a tanúsítványszolgáltatásokra és az archiválásszolgáltatásra is, melyek szintén a megelőző, összes minősített bizalmi szolgáltatást tartalmazó tervezet alapján készültek.	Szabó Zoltán Varga Viktor
1.3.6.1.4.1.3555.1.16.20170515	nem hatályosított verzió	A Szolgáltató minősített bizalmi szolgáltatásait vizsgáló megfelelőségértékelési eljárás során a megfelelőségértékelő szervezettel történt informatív egyeztetések alapján a 20170427-es verziót pontosító és kiegészítő verzió, mely a Szolgáltató weboldalán jóváhagyásának napján nyilvános tervezetként közzétételre került. A minősített tanúsítványszolgáltatások bizalmi felügyelethez történő bejelentéshez Szolgáltató szintén e verziót csatolta. (Az eIDAS 20. cikk (1) bekezdés szerinti megfelelőség értékelési eljárást az eIDAS 3. cikk 18. pont szerinti megfelelőségértékelő szervezetként a MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft.	Szabó Zoltán Varga Viktor

		végezte 2017 májusában.)	
1.3.6.1.4.1.3555.1.16.20170615	2017. június 19-től visszavonásig vagy új verzió hatálybalépéséig	A Szolgáltató minősített bizalmi szolgáltatásait vizsgáló megfelelőségértékelési eljárást záró szakterületi jelentésekben a megfelelőségértékelő szervezet által megfogalmazott javaslatok végrehajtásával a 20170515-ös verzióból készített új verzió.	Szabó Zoltán

1.3 A PKI szereplők

Jelen Szolgáltatási Rend keretében a PKI szereplők alatt az időbélyeg-szolgáltatás Ügyfeleit (Igénylőit és Előfizetőit), Végfelhasználóit, a Szolgáltatót és szervezeti egységeit, valamint az Érintett feleket kell érteni.

Lásd még az 1.6.1 Fogalmak fejezet releváns fogalom meghatározásait.

1.3.1 A Szolgáltató

Szolgáltató a bizalmi minősített időbélyeg-szolgáltatás keretében az RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol szerinti időbélyegeket kibocsátását biztosítja Végfelhasználók számára.

1.3.2 Előfizető, Végfelhasználó és Igénylő

Előfizető és Igénylő a Szolgáltató Ügyfelei, akikkel Szolgáltató szerződéses kapcsolatba kerül. Végfelhasználó személyét az Előfizető határozza meg.

Lásd még a 1.6 Fogalmak és rövidítések fejezet vonatkozó fogalom magyarázatait.

1.3.4 Érintett felek

Az Érintett felek jellemzően nem állnak szerződéses kapcsolatban a Szolgáltatóval, de részükre a jelen Szolgáltatási Rend alapján készült szolgáltatási szabályzat ajánlásokat fogalmazhat meg az általuk igénybevett - jellemzően - nem díjköteles szolgáltatások - jellemzően az időbélyegek ellenőrzéséhez igénybevett tanúsítvány-állapotszolgáltatások - kapcsán. A Szolgáltató az Érintett Felekkel elsősorban a tanúsítványtáron keresztül tart kapcsolatot.

Lásd még az 1.6.1 fejezet Érintett Fél fogalmát.

1.3.5 Egyéb szereplők

Nincs megkötés.

1.4 Időbélyegek alkalmazhatósága

Szolgáltató által kibocsátott időbélyeg alkalmas az időbélyegzővel ellátott elektronikus dokumentum adott formában való létezésének hiteles igazolására Érintett felek számára.

1.5 A Bizalmi Szolgáltatási Rend adminisztrációja

A Szolgáltató Bizalmi Szolgáltatási Rendjének kibocsátását, karbantartását a Szolgáltató szabályzatért felelős egysége végzi.

A Szabályzatelfogadó Egység állandó tagjai a Szolgáltató munkatársai, akiket a Szolgáltató Ügyvezetése írásban jelöl ki. Az Egység működését a Szabályzatelfogadó Egység belső, nem nyilvános működési szabályzata írja le.

A Szolgáltató szabályzatainak módosításával kapcsolatban lásd a 9.12 fejezetet.

1.5.1 A dokumentum adminisztrációját végző szervezet

A Szolgáltató szabályzatokért (kikötésekért) felelős egységének neve NETLOCK Szabályzatelfogadó Egység. A Szabályzatelfogadó Egység állandó tagjai a Szolgáltató munkatársai, akiket a Szolgáltató Ügyvezetése írásban jelöl ki. Az Egység működését a Szabályzatelfogadó Egység belső, nem nyilvános működési szabályzata írja le.

A Szolgáltató szabályzatainak módosításával kapcsolatban lásd a 9.12 fejezetet.

1.5.2 A dokumentum kapcsolattartó személye

Jelen dokumentummal kapcsolatban a Szabályzatelfogadó Egység kapcsolattartásért felelős személye a jelen dokumentum jóváhagyója (lásd a dokumentum fedlapját).

Jelen dokumentummal kapcsolatos kérdésekkel és észrevételekkel az Ügyfelek, a Végfelhasználók és az Érintett felek elektronikus levélben az szee@netlock.hu címen kereshetik meg a NETLOCK Szabályzatelfogadó Egységét.

Szolgáltató munkatársai észrevételeiket egyéb csatornán keresztül is, de szintén csak írásban juttathatják el a Szabályzatelfogadó Egységhez.

A Szabályzatelfogadó Egységnek elektronikus levélben küldött megkeresések (lásd 1.5.1) megválaszolásáért illetve - amennyiben szükséges az észrevétel nyomán megtenni szükséges egyéb intézkedések megtételéért a kapcsolattartó személy felelős.

A Szabályzatelfogadó Egység részére jelen dokumentummal kapcsolatban eljuttatott kérdés vagy észrevétel esetén a kapcsolattartónak kell kijelölnie az Egység azon munkatársát, aki a megkeresést feldolgozza. Összetettebb tárgyú megkeresés esetén összehívja a Szabályzatelfogadó Egység ülését - az Egység szabályzatában foglaltaknak megfelelően.

A megkeresés feldolgozása során, az Egység vagy munkatársa azonosítja a dokumentum észrevétellel, kérdéssel érintett pontját/pontjait, majd az Egység többi munkatársával egyeztetve - és szükség esetén más munkatársak véleményét is kikérve - küld választ elektronikus levélben az értesítést küldőnek.

Amennyiben a megkeresés nyomán jelen Szolgáltatási Rend vagy más dokumentum módosítása szükségessé válik, a módosítással kapcsolatban a 9.12 fejezet szerint kell Szolgáltatónak eljárnia.

1.5.3 A szolgáltatási szabályzat szolgáltatási rendnek megfelelésért felelős szervezet

A jelen Szolgáltatási Rend alapján nyújtott minősített időbélyeg-szolgáltatás nyújtásának és

igénybevételének részletes gyakorlati előírásait tartalmazó Szolgáltatási Szabályzat Szolgáltatási Rendnek való megfelelését a NETLOCK Szabályzatelfogadó Egység ellenőrzi. A jelen Szolgáltatási Rend alapján készült szolgáltatási szabályzatot a Szabályzatelfogadó Egység a jelen Szolgáltatási Rendnek való maradéktalan megfelelés esetén hagyhatja jóvá.

A Szolgáltatási rend vagy nyilvános tervezete közzétételének feltétele, annak jóváhagyása.

1.5.4 A Szolgáltatási szabályzat elfogadása

A jelen Szolgáltatási Rendnek megfelelő Szolgáltatási Szabályzat elfogadási eljárását Szolgáltatónak ismertetnie kell a szolgáltatási szabályzatban.

A Szolgáltatási Rend módosításával kapcsolatban lásd a 9.12 fejezetet.

1.6 Fogalmak és rövidítések

1.6.1 Fogalmak

AIA	CAI (Authority Information Access:Certificate Authority Issuers): Az adott tanúsítvány kiadói tanúsítványára vonatkozó elérhetőséget (URL) tartalmazó tanúsítványmező.
Alárendelt szolgáltatás	Szolgáltató szabályzatai alapján működő nem minősített bizalmi szolgáltatás, mely számára Szolgáltató biztosít tanúsítványt.
Aktiváló adat	Olyan a szolgáltató által előállított vagy végfelhasználó által megadott, kizárólag a végfelhasználó által ismert kódsorozat (jelszó, PIN kód), ami a magánkulcsot alkalmazásra képes állapotba helyezi. Tanúsítványaktiváláshoz nincs köze.
Aláírás	Lásd elektronikus aláírás
Aláírás / Bélyegző Létrehozó eszköz	Olyan kriptográfiai eszköz, amely minősített aláírás / bélyegző létrehozására nem alkalmas (lásd még 1.6.2. Rövidítések, SCD).
Aláírási szolgáltatás	Az eIDAS szerinti alábbi szolgáltatások: ● elektronikus aláírások és elektronikus bélyegzők létrehozása, ellenőrzése és érvényesítése, ● valamint ezekhez kapcsolódó tanúsítványok ellenőrzése és érvényesítése. Jelen szabályzat keretében e szolgáltatások “felhőalapú” nyújtását értjük, a végfelhasználói aláíró és bélyegző kulcsok szolgáltató által tárolásával és az ügyfelek által webes felületen/protokollon keresztül feltöltött dokumentumok aláírásával/bélyegzésével (beleértve opcionálisan az időbélyeg elhelyezését is).
Aláírói partner	Szolgáltatói partner, aki az aláírási szolgáltatást saját ügyfelei számára biztosítja, amelynek részeként részt vehet a Végfelhasználók azonosításában (akik tekintetében korlátozott információs és adminisztrációs jogokkal bír), s aki az aláírási szolgáltatást saját szolgáltatásával integráltan szolgáltatás nyújtására használja, s aki Előfizetőként vállalja a díjfizetést a végfelhasználók után.

Alany	Lásd az Eüt. 1. § 43. pontjának meghatározását. Jelen szabályzat keretében a tanúsítvány Subject és SAN mezőit, illetve az ezekben feltüntetésre kerülő adatokat értjük alatta, amelyek utalhatnak egy természetes személyre és/vagy egy szervezetre és/vagy egy védjegyre/terméknévre vagy egy eszköz/rendszer azonosítójára/más elnevezésére vagy egy álnévre. Lásd az Igénylő, Előfizető, Ügyfél és Végfelhasználó entitásokat.
Állapotváltoztatás	Az az eljárás, aminek eredményeként a tanúsítvány állapota (érvényes, felfüggesztett) megváltozik és új értéket vesz fel (érvényes, felfüggesztett, visszavont).
Archiválási szolgáltatás	Az Eüt. 1. § 2 szerint: “Az elektronikus dokumentumok hosszú távú megőrzésére vonatkozó szolgáltatás, amely magában foglalja az eIDAS Rendelet 3. cikk 16. pont c) alpontja szerinti bizalmi szolgáltatást is”. Jelen szabályzat keretén belül olyan minősített bizalmi szolgáltatás, mely során a Bizalmi Szolgáltató a hozzá archiválás céljából eljuttatott elektronikusan hitelesített (aláírt vagy bélyegzett) dokumentumok aláírása vagy bélyegzője teljes érvényességi láncát létrehozza vagy kiegészíti, az érvényességi láncot archív időbélyeggel ellátja, majd az így kiegészített dokumentumot vagy fájlt biztonságosan eltárolja.
Átvevő	A végfelhasználó valamely kulcsát vagy eszközét (pl. Ügyféleszköz) és aktiváló adatát Szolgáltatótól (személyesen, hagyományos vagy elektronikus kézbesítés útján) átvevő személy, aki az lehet, aki az adott tanúsítvány esetében Igénylő lehet.
Bélyegző	Lásd elektronikus bélyegző
Bizalmi lista	Hatóság vagy szoftvergyártó által kezelt lista, amely a megbízhatónak tartott bizalmi szolgáltatások azonosítóit (jellemzően tanúsítványait) tartalmazza. Egy adott bizalmi listát kezelő szoftver a benne lévő szolgáltatásokra visszavezethető aláírásokat, bélyegzőket és időbélyegzőket elfogadja. Jellemzően az EU bizalmi listát értjük alatta, ahol az eIDAS szerinti nem minősített és minősített szolgáltatások kerülnek feltüntetésre az egyes tagországok felügyeleti szervei által. Lásd: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-certification-service-providers
Bizalmi Szolgáltatási Rend	NETLOCK Bizalmi Szolgáltatási Rend Minősített Tanúsítványszolgáltatásra
Bizalmi Felügyelet	Az Eüt. által a bizalmi szolgáltatások felügyeletére kijelölt szerv. Konkrétan a Nemzeti Média- és Hírközlési Hatóság.
Bizalmi munkakör	A szolgáltató informatikai rendszeréért általánosan felelős vezetői munkakör. Lásd az 5.2.1 Bizalmi munkakörök fejezetet.
Bizalmi munkatárs	A Szolgáltatónál vagy Szolgáltatói partnerénél bizalmi munkakört betöltő személy.

Bizalmi szolgáltatás	Az eIDAS 3. cikk 16. Pontja szerint: “Rendszerint díjazás ellenében nyújtott, jelen Szabályzat keretében az alábbiakból álló elektronikus szolgáltatások: - elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy - weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése.” Jelen szabályzat keretén belül a Szolgáltató elektronikus aláírásokhoz, elektronikus bélyegzőkhöz és weboldal hitelesítéshez kapcsolódó, a tanúsítványok kibocsátását és életciklusmenedzsmentjét biztosító, valamint az Időbélyegző szolgáltatását értjük alatta.
Biztonságos zóna:	Olyan (logikailag vagy fizikailag) védett terület, amely védi a titkosságát, integritását és elérhetőségét a Szolgáltató által használt rendszereknek.
CAA ellenőrzés	Olyan ellenőrzés, amikor a DNS bejegyzésben RFC 6844 szerinti CAA rekordokat keres a Szolgáltató. Ha itt arra utaló bejegyzés van, hogy más Szolgáltatóval tart kapcsolatot a domaintulajdonos, akkor nem adható ki tanúsítvány.
Eakta (formátum)	Elektronikus aláírás konténerformátum, amely dokumentumokat, illetve hozzájuk kapcsolódó profilokat (metaadatokat), aláírásokat, ellenjegyzéseket és időbélyegzőket tartalmazhat, szabványos, az ETSI TS 101 903 (XAdES) specifikációnak megfelelően. Lásd bővebben: https://e-szigno.hu/tudasbazis/e-akta-formatum-specifikacioja.html
EV tanúsítvány Extended Validation Certificate (EVC)	Olyan weboldal-hitelesítő tanúsítvány, ami megfelel az EVCG követelményeinek.
Elektronikus aláírás	Olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ (eIDAS 3 cikk 10. pont). Jelen szabályzat keretén belül: A Szolgáltató által kibocsátott aláíró tanúsítvány magánkulcs párjával természetes személy által létrehozott elektronikus adat, amelyet az aláírandó elektronikus dokumentumhoz (vagy más elektronikus adatokhoz) csatolnak, s ami a tanúsítvánnyal és a benne foglalt nyilvános kulccsal ellenőrizhető.
Elektronikus bélyegző	Olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét. Az elektronikus aláírás jogi személy által létrehozott megfelelője.
Előfizető	Szolgáltató azon szerződéses partnere, aki a szolgáltatási díjak fizetését vállalja. Jogai és kötelezettségei az ÁSZF-ben és a Szolgáltatási szerződésben elkülönülten megjelennek. Tanúsítványszolgáltatás esetén amennyiben a tanúsítvány

	Alanyként szervezet is megnevezésre került vagy csak egy természetes személy van benne megnevezve, akkor jellemzően azzal megegyezik. NL Sign szolgáltatás esetén megegyezik az Aláírói Partnerrel vagy a Végfelhasználóval. Lásd még az Ügyfél, Igénylő és Végfelhasználó entitásokat, valamint az 1.3.3 Előfizető, Végfelhasználó és Igénylő fejezetet.
Érintett fél	Természetes vagy jogi személy, aki Szolgáltatóval nem kerül szerződéses kapcsolatba, de annak valamely - jellemzően ingyenes - tanúsítvány állapot szolgáltatását igénybe veszi (pl. elektronikus aláírást, bélyegzőt vagy időbélyegzőt ellenőriz és ennek kapcsán az egyes tanúsítványok érvényességi információit vagy szolgáltató szabályzatait ellenőrzi). Lásd az 1.3.4 Érintett felek fejezetet.
Érvényes tanúsítvány	Olyan tanúsítvány, amelynek az érvényességi idejébe esik a mindenkori jelen időpont, és amelynek állapota nem felfüggesztett vagy visszavont (lásd Tanúsítványállapot).
Érvényességi idő(tartam)	Egy kezdeti és végső időpont közötti időtartam, amelyre a tanúsítvány kiadásra került.
Eszközös tanúsítvány	Olyan tanúsítvány, aminek magánkulcsa Kriptográfiai eszközre kerül kiadásra.
Érvényességi lánc	Az elektronikus dokumentum vagy annak lenyomata és azon egymáshoz rendelhető információk (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás vagy bélyegző létrehozásához használt adatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató érvényességi adatára és annak visszavonására vonatkozó információk) sorozata, amelyek segítségével megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás, bélyegző vagy időbélyegző, az aláírás, bélyegző vagy időbélyegző elhelyezésének időpontjában érvényes volt. Általánosabb értelemben egymást hitelesítő tanúsítványok hierarchiája, egészen a gyökér tanúsítványig.
Fokozott biztonságú elektronikus aláírás	Olyan elektronikus aláírás, amely megfelel az eIDAS 26. cikkben meghatározott követelményeknek.
Fokozott biztonságú elektronikus bélyegző	Olyan elektronikus bélyegző, amely megfelel az eIDAS 36. cikkben meghatá-rozott követelményeknek.
Hitelesítési rend	Az Eüt. 1. § 24 szerint: olyan bizalmi szolgáltatási rend, amely bizalmi szolgáltatás keretében kibocsátott tanúsítványra vonatkozik. Szolgáltató szabályzati keretében egy szabványos eljárásrend, ami alapján Szolgáltató tanúsítványt bocsát ki és kezel. Szolgáltató szabályzatai több hitelesítési rendet is magukban foglalnak, megkülönböztetve a nekik megfelelő követelményeket és eljárásokat.

Hitelesítő egység	Szolgáltató szervezeti egysége, amely a Regisztrációs egység kérelme alapján a tanúsítványok kiadását, publikálását, visszavonását, felfüggesztését, valamint a Tanúsítványvisszavonási lista publikálását végzi. Lásd az 1.3.1 fejezetet.
Hitelesítési Ügyintéző	A Hitelesítő Egységen belül e munkakörben dolgozó munkatársak a tanúsítványok kibocsátásának jóváhagyását végzik.
Hozzáférő	Az archiválásszolgáltatás Előfizetőjének kezdeményezésére a szolgáltatás bizonyos funkcióit a kezdeményező Előfizető által meghatározott dokumentumok tekintetében díjmentesen elérő Érintett fél. Lásd az 1.3.5 Érintett felek fejezetet.
Igénylő	Tanúsítványszolgáltatás esetén a tanúsítványkibocsátási tanúsítványkezelési és állapotváltoztatási eljárásban eljáró, a szolgáltatói szerződést Ügyfél részéről elfogadó természetes személy, aki lehet: ● a tanúsítvány Alanyaként megjelölt természetes személy (Álnév esetén az álnév kérelmezője); ● ennek hiányában a tanúsítvány Alanyaként megjelölt szervezet képviselője vagy meghatalmazottja; ● ezek hiányában a tanúsítvány Alanyaként megjelölt domain név, trademark vagy terméknév tulajdonosa, ill. szervezet tulajdonos esetén annak képviselője vagy meghatalmazottja, illetve a domain név fölött kontrollal rendelkező személy. Előfizetővel megegyezik, amennyiben a tanúsítvány Alanyaként egy természetes személy kerül feltüntetésre (és szervezetnem). NL Sign szolgáltatás esetén megegyezik Végfelhasználóval. Archiválás- és Időbélyegszolgáltatás esetén megegyezik Előfizetővel.
Időbélyegző	Olyan elektronikus adat, amely más elektronikus adatokat egy adott időponthoz köt, amivel igazolja, hogy utóbbi adatok léteztek az adott időpontban.
Időbélyegző Kiszolgáló	A Szolgáltató időbélyegzőket kibocsátó műszaki rendszere.
Időbélyegző szolgáltatás	Szolgáltató azon szolgáltatása, amely a számára küldött elektronikus adatok lenyomata alapján egy időbélyegzőt állít elő, az adott adatokhoz.
Időbélyeg-URL	Az időbélyeg-szolgáltatás elérését biztosító, az Előfizető egyedi azonosítóját tartalmazó virtuális token, melyen keresztül Végfelhasználó időbélyeg kéréseket továbbíthat Szolgáltató felé, Szolgáltató pedig a kérés alapján időbélyeg választ továbbít Végfelhasználó felé.
Kézbesítési Megbízott	Olyan Szolgáltatói partner, aki Szolgáltató megbízásából - Igénylő ilyen irányú igénye esetén - az Igénylővel egyeztetett helyen és időben végzi el a Tanúsítványkibocsátáshoz kapcsolódóan az ügyféleszköz átadását.

KGyHSz	Közigazgatási Gyökér Hitelesítésszolgáltató Lásd 1.3.5 és http://www.kgyhsz.gov.hu/
Központi Regisztrációs Egység	A Szolgáltató azon saját szervezetén belül működtetett szervezeti egysége, mely feldolgozza a szolgáltatások igényléseit, azonosítja azok Igénylőjét és Előfizetőjét, ellenőrzi az eljárási jogukat és adataikat.
Kezdeti felfüggesztés	A Tanúsítványfelfüggesztés egy speciális esete, amikor a Szolgáltató a tanúsítványt kibocsátása után azonnal felfüggeszti, így megóvva azt a visszaélésektől arra az időszakra, míg a Tanúsítvány és a magánkulcs biztonságosan eljut az Ügyfélhez.
Képviseleti jog	Teljes vagy részleges képviseleti jog vagy ekként is értelmezhető jogviszony (lásd Eüt. 82. § (9)).
Kiadó	Szolgáltató tanúsítványokat kibocsátó műszaki rendszere. Szolgáltatónál létezik végfelhasználói és egyes szolgáltatói tanúsítványokat kibocsátó Köztes Kiadó, valamint az ezen egységeket hitelesítő legfelső szintű Gyökér Kiadó, amelyek hierarchiába szervezetten működnek.
Kihelyezett Hitelesítő Egység	A Szolgáltatótól független, önálló szervezet vagy személy (mint Szolgáltatói partner) által, a Szolgáltató előírásai alapján működtetett Hitelesítő Egység.
Kihelyezett Regisztrációs Egység	A Szolgáltatótól független, önálló szervezet vagy személy (mint Szolgáltatói partner) által, a Szolgáltató előírásai alapján működtetett Regisztrációs Egység.
Kikötések (és feltételek)	Szolgáltató azon dokumentumai, amelyek ismertetik, hogy a szolgáltatások nyújtásával kapcsolatosan, milyen elvárásoknak, milyen módon felel meg, s ismertetik a többi szereplő kötelezettségeit és jogait. Ide tartozik a Szolgáltató Szolgáltatási kivonata, Hitelesítési rendje, Szolgáltatási szabályzata, ÁSZF-e, szolgáltatási szerződése, valamint a közöttük létrejött egyéb megállapodások együttesen.
Kriptográfiai eszköz	Olyan biztonságos hardver eszköz, amely a Végfelhasználó magánkulcsát tartalmazza, azt védi a kompromittálódás ellen, s a kulccsal kriptográfiai műveleteket (pl. aláírás, titkosítás) végez a Végfelhasználó számára. Lehet SCD és QSCD, HSM vagy más nem aláírás célú eszköz is. Lehet a Szolgáltató vagy az Ügyfél kezelésében. Utóbbi esetben “Ügyféleszközként” hivatkozunk rá.
Kritikus szolgáltatások	A Szolgáltató tanúsítvány- és kulcselőállítással, az Ügyfelek eszközzel való ellátásával és az állapotváltoztatással kapcsolatos szolgáltatásai.
Kulcscsere	Az a folyamat, amikor a Szolgáltató egy már regisztrált Ügyfél (vagy saját maga) részére bocsát ki új Tanúsítványt és magánkulcsot, annak egy már létező tanúsítványát alapul véve. Az új tanúsítványban a végfelhasználó nyilvános kulcsa megváltozik.

	Lásd a 4.7 fejezet.
Kulcsletét szolgáltatás	Olyan szolgáltatás, amely a végfelhasználó magánkulcsának megőrzését és annak végfelhasználó számára történő átadását biztosítja (arra az esetre, ha a végfelhasználó kulcs elveszne, megsemmisülne vagy más okból használhatatlanná válna).
Magánkulcs	A szolgáltató vagy ügyfél által generált kulcspár egyik kulcsa, amit végfelhasználó kezel. Lásd nyilvános kulcs. Amennyiben a nyilvános kulcs aláíró vagy bélyegző tanúsítványba kerül, akkor megfelel az eIDAS elektronikus aláírás létrehozásához használt adat és elektronikus bélyegző létrehozásához használt adatok definíciójának.
Minősített Aláírás / Bélyegző Létrehozó eszköz	Olyan kriptográfiai eszköz, amely minősített aláírás / bélyegző létrehozására alkalmas (lásd még 1.6.2. Rövidítések, QSCD).
Minősített tanúsítvány	Olyan tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel az eIDAS Annex I, III vagy IV részének vagy a 1999/93/EC direktívának, attól függően, hogy a tanúsítvány kiadásakor melyik volt hatályban.
Minősített weboldal hitelesítő tanúsítvány	Az eIDAS 3. cikk 39. Pontja szerint: “Olyan weboldal-hitelesítő tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel az eIDAS IV. mellékletben megállapított követelményeknek.” Olyan minősített tanúsítvány, amely a benne megjelölt weboldalak hitelesítésével biztosítja az oldal látogatóit, hogy a mögött egy valódi és legitim szervezet áll.
Mobil Regisztrációs Munkatárs	Olyan regisztrációs ügyintéző, aki - amennyiben személyes találkozó szükséges - az Igénylő azonosítását - ilyen irányú igénye esetén - az Igénylővel egyeztetett helyen és időben végzi el.
NL Sign szolgáltatás	Biztonságos központi kulcstárolási (menedzselt SCD) és kulcsmenedzsment-szolgáltatás, mely webes felületen keresztül feltöltött dokumentumok elektronikus aláírását/bélyegzését (és időbélyegzését) teszi lehetővé. Az NL Sign szolgáltatás keretében használható tanúsítványok igénylése és az ehhez szükséges regisztrációs adatok bekérése valamint a tanúsítvány kibocsátását követően annak használatba vétele az NL Sign szolgáltatás webes felületein történik.
Nyilvános kulcs	A szolgáltató vagy ügyfél által generált kulcspár egyik kulcsa, amit szolgáltató az általa létrehozott tanúsítványban helyez el. Lásd magánkulcs.
Permanens azonosító	Olyan azonosító, mely a tanúsítvány birtokosát egyedileg azonosítja. A tanúsítványban történő megvalósítása az RFC 4043 alapján történik. Lehet szolgáltató által képzett, vagy hivatalos nyilvántartásban szereplő egyedi azonosító adat. A szolgáltató által képzett azonosító egy OID, ami két részből áll: a Szolgáltató (1.3.6.1.4.1.3555) és az Ügyfél egyedi azonosítójából, ami ezt

	követi. Az Ügyfél egyedi azonosítója 5-tel kezdődik, amelyet egy szám követ, ami a következő értékeket veheti fel: ● 1,6,8,10: személyes vagy üzleti tanúsítványok esetén, amikor az azonosító a természetes személy adataiból képzett. ● 2,7,9,11: szervezeti tanúsítványok esetén, amikor az azonosító a szervezet adataiból képzett. Alkalmazása esetén a tanúsítvány Subject/SerialNumber mezőjébe kerül.
Regisztráció	Kezdeti azonosítási eljárás, amelyet Szolgáltató Igénylő és Előfizető személyazonosságának megállapítására, eljárási joguk ellenőrzésére, valamint adatainak felvételére végez.
Regisztrációs egység	A Szolgáltató azon egysége, amely a szolgáltatások igénylésének feldolgozását, az Igénylő és Előfizető regisztrációját, valamint tanúsítványszolgáltatás esetén a tanúsítványba kerülő adatok ellenőrzését végzi. Létezhet a Szolgáltatón belül (mint belső szervezeti egység) vagy kívül (Kihelyezett Regisztrációs Egység) egyaránt.
Regisztrációs felelős	Bizalmi munkakör. Lásd az 5.2.1 Bizalmi munkakörök fejezetet.
Regisztrációs (és visszavonási) ügyintéző	Szolgáltató Regisztrációs egységén belül e munkakörben dolgozó munkatársak feladata a tanúsítványigénylések kezelése és a tanúsítványigénylésben megadott adatok valódiságának ellenőrzése (lásd 4.2.1 fejezet) valamint a visszavonási igények feldolgozása és végrehajtása (4.9).
SSL tanúsítvány	Weboldal-hitelesítő tanúsítvány
Szervezet	Tanúsítvány alanya vagy előfizetője tekintetében: jogi személy vagy egyéni vállalkozó vagy egyéni ügyvéd.
Szoftveres tanúsítvány	Olyan tanúsítvány, aminek magánkulcsa nem Kriptográfiai eszközre kerül kiadásra.
Szolgáltatás	Jelen szabályzat keretén belül Szolgáltató bizalmi szolgáltatásai (lásd 1.1 fejezet).
Szolgáltatási Szabályzat	A bizalmi szolgáltató nyilatkozata az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről (lásd Eüt. 1. § 41.), mely Szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmaz.
Szolgáltatási szerződés	Szolgáltató és Ügyfél között létrejött szerződés, amely a szolgáltatás nyújtására és igénybevételére vonatkozó feltételeket tartalmazza. Megkötése a szolgáltatás igénybevételének előfeltétele.
Szolgáltató	Jelen Bizalmi Szolgáltatási rend szerinti bizalmi és nem bizalmi szolgáltatásokat nyújtó NetLock.
Szolgáltató szabályzatai	Jelen Bizalmi Szolgáltatási Rend, a Bizalmi Szolgáltatási Szabályzat, az ÁSZF, a szolgáltatási szerződés, a Szolgáltatási kivonat.

	Valamint egyéb nem nyilvános szabályzatok.
Szolgáltatói partner	Olyan a szolgáltatótól független, önálló természetes vagy jogi személyek, amelyek a Szolgáltatóval való megállapodás alapján a Szolgáltatás nyújtásában részt vesznek.
Szolgáltatói rendszer	Szolgáltató szolgáltatásnyújtást végző rendszereinek együttese.
Szolgáltatói tanúsítvány	Szolgáltató azon tanúsítványai, amelyeket a szolgáltatásnyújtás érdekében használ (pl. Kiadók és Időbélyegző Kiszolgálók tanúsítványai).
Tanúsítvány	Szolgáltató által kibocsátott hiteles igazolás, amely a nyilvános kulcsot az Alanyhoz kapcsolja, és igazolja e Tanúsítványban közzétett adatok valódiságát.
Tanúsítványaktiválás	Az az állapotváltoztatási eljárás, amely felfüggesztett tanúsítvány érvényességét visszaállítja. Aktiválása után a tanúsítvány visszamenőlegesen, azaz a felfüggesztés időtartamára is újra érvényessé válik, mintha a felfüggesztés meg sem történt volna.
Tanúsítványállapot	A szolgáltató által a tanúsítványok érvényességi ideje alatt nyilvántartott érvényes / visszavont / felfüggesztett státusza, amelyről a tanúsítvány-visszavonási listán és a Tanúsítványállapot szolgáltatáson keresztül ad tájékoztatást Ügyfelei és az Érintett felek részére.
Tanúsítványállapot-szolgáltatás (OCSP)	Olyan szolgáltatás, ami egy adott tanúsítvány állapotáról ad valós idejű információt az érintett felek számára. Lásd még: tanúsítvány visszavonási lista.
Tanúsítványfelfüggesztés	Az az állapotváltoztatási eljárás, amelyben a Szolgáltató egy még érvényes Tanúsítvány érvényességét átmenetileg megszünteti az eredetileg tervezett érvényességi idő vége előtt. A tanúsítványfelfüggesztés egy átmeneti állapot, a felfüggesztett Tanúsítvány visszavonható, vagy a Tanúsítvány eredeti érvényességi idejében újra érvényessé tehető. A felfüggesztés visszavonása esetén a Tanúsítvány visszamenőleges hatállyal érvényessé válik, mintha a felfüggesztés meg sem történt volna.
Tanúsítványigénylés	Az a folyamat, amikor Igénylő tanúsítványt igényel, azaz a tanúsítvány elkészítéséhez szükséges adatokat megadja és igazolja a Szolgáltatónak, végül pedig Szolgáltatási szerződés Igénylő és - amennyiben nem egyezik Igénylővel - Előfizető általi aláírásával hitelesíti kérelmét az igényelt tanúsítványra vonatkozóan és ezzel felhatalmazza Szolgáltatót az igényelt tanúsítvány kibocsátására.
Tanúsítványkezelési eljárás	Olyan eljárás, ami új tanúsítvány kibocsátását eredményezi egy meglévő tanúsítvány illetve korábbi ügyfél-regisztráció adatai alapján (lásd 3.3 Azonosítás és hitelesítés tanúsítványkezelési eljárás során és 4. Életciklus követelmények fejezeteket).
Tanúsítványszolgáltatás	Szolgáltató azon szolgáltatása, amelynek keretén belül új tanúsítványt állít elő. Ez történhet egy már létező tanúsítvány alapján (követő kibocsátás tanúsítványkezelési eljárással) vagy ilyen előzmények nélkül (eredeti kibocsátás).

Tanúsítványmegújítás	Az a folyamat, amikor a Szolgáltató ugyanarra a nyilvános kulcsra, változatlan Alannyal egy új Tanúsítványt állít ki, új érvényességi időszakra. Lásd a 4.6 fejezet.
Tanúsítványmódosítás	Az a folyamat, amikor a Szolgáltató egy már regisztrált Igénylő részére bocsát ki új Tanúsítványt egy korábban kibocsátott Tanúsítványa alapján, az abban szereplő nyilvános kulccsal, de megváltozott Alany vagy Szolgáltató adatokkal. Lásd a 4.8 fejezet.
Tanúsítványtár	Szolgáltató kibocsátott tanúsítványokat tartalmazó nyilvántartása, amelyen keresztül lekérdezhetők a szolgáltató által kiadott nyilvános tanúsítványok és a Tanúsítványvisszavonási lista.
Tanúsítványtípus	Szolgáltató által kibocsátott különböző tanúsítványok megkülönböztetése valamilyen jellemző szerint, legfőképpen a felhasználási cél alapján. Lásd a Szolgáltatási szabályzat 1.2.1 pontját.
Tanúsítvány-visszavonás	Az az állapotváltoztatási eljárás, amelyben a Szolgáltató a tanúsítvány érvényességét megszünteti az eredetileg tervezett érvényességi idő lejárta előtt. A tanúsítvány-visszavonás visszafordíthatatlan és végleges állapotváltozást jelent, a visszavont tanúsítvány a visszavonás időpontjában érvényességét veszti, s már soha többé nem lehet újra érvényes.
Tanúsítványvisszavonási lista (CRL)	Szolgáltató által rendszeres időközönként, valamint állapotváltozások hatására a Tanúsítványtárban közzétett hiteles lista azon tanúsítványokról, amelyek ideiglenesen vagy véglegesen nem érvényesek. A listán szereplő tanúsítványok elfogadása, illetve alkalmazása nem ajánlott. A 24/2016. BM rendelet 17. szerinti visszavonási nyilvántartás egy fajtája.
Teszttanúsítvány	A Szolgáltató által tesztelési célra kibocsátott tanúsítvány, ami tartalmában valamely valódi tanúsítvánnyal egyezik meg, de hitelesítési rend mezője és az Alany elnevezése jelzi a felhasználás teszt voltát. Az ilyen tanúsítványok kötelezettségvállalásra nem használhatók, joghatás nem kapcsolódik hozzájuk, elfogadásuk csak tesztelési céllal lehetséges. Szolgáltató nem vállal felelősséget az ilyen tanúsítványok adattartalma, felhasználása, és a hozzájuk kapcsolódó szolgáltatások rendelkezésre állása tekintetében.
UCC weboldal-hitelesítő tanúsítvány	Olyan weboldal-hitelesítő tanúsítvány, melyben több különböző domain név kerül feltüntetésre (a SubjectAltName/DNSname mezőben).
Ügyfélmenü	A Szolgáltató ügyfelei számára a tanúsítványokkal és hozzájuk kapcsolódó szolgáltatásokkal kapcsolatos különböző igénylések elvégzésére illetve a folyamatban lévő igénylések állapotának megtekintésére biztosított, a Szolgáltató weboldalán keresztül elérhető felület, melybe egyedi felhasználónév és jelszó megadásával lehet belépni (ügyfélmenü regisztrációt követően). A minősített tanúsítványok kezeléséhez a minősített ügyfélmenübe, a nem-minősített tanúsítványok kezeléséhez a fokozott biztonságú ügyfélmenübe kell regisztrálni és bejelentkezni.

Ügyfélmenü regisztráció	Az a folyamat, amikor egy természetes vagy jogi személy adatai megadásával létrehozza saját Ügyfélmenüjét, illetve az Ügyfélmenübe való bejelentkezéshez szükséges bejelentkező nevét és jelszavát.
Ügyfél	A Szolgáltatatóval szerződést kötő fél. Tanúsítványszolgáltatás esetén a tanúsítvány Igénylője és Előfizetője (adott esetben ezek a szereplők meg is egyeznek). NL Sign szolgáltatás esetén az Aláírói Partner és a Végfelhasználó. Lásd még az 1.3.3 Előfizető, Végfelhasználó és Igénylő fejezetet
Ügyféleszköz	Lásd Kriptográfiai eszköz.
Ügyfél-regisztráció	Természetes és nem természetes személyek azonosítása, adataik ellenőrzése és rögzítése az első szolgáltatási szerződés és az első tanúsítványkibocsátás megelőzően. Lásd a 3.2 Kezdeti azonosítás fejezetet.
Végfelhasználó	Az a természetes személy, aki a tanúsítványban szereplő nyilvános kulcs magánkulcs párja felett rendelkezik (kizárólagosan használja vagy a használatáért felelős). NL Sign szolgáltatás esetén az a személy, aki az aláírási szolgáltatás keretén belül a magánkulcsa aktiválásával elektronikus aláírási/bélyegző műveletet hajt végre, illetve aki e műveletekért felelős. Lásd még az Ügyfél és Előfizető entitásokat, valamint az 1.3.3 Előfizető, Végfelhasználó és Igénylő fejezetet
Végfelhasználói tanúsítvány, Végfelhasználói kulcs	Az Előfizetők tanúsítványát és kulcsát jelöli, megkülönböztetve a Szolgáltató saját tanúsítványaitól és kulcsaitól.
Weboldal-hitelesítő tanúsítvány	Az eIDAS 3. cikk 38. pontja szerinti tanúsítvány.
Wildcard weboldal-hitelesítő tanúsítvány	Olyan weboldal-hitelesítő tanúsítvány, melyet több aldomain hitelesítésére bocsátott ki szolgáltató (a domain név *.domain.hu formában kerül feltüntetésre, így magában foglalja a domain.hu cím alá tartozó valamennyi aldomaint).

1.6.2 Rövidítések

Hivatkozott jogszabályok rövidítései

eIDAS	Az Európai Parlament és Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről.
Eüt.	Az elektronikus ügyintézés és a bizalmi szolgáltatások általános

	szabályairól szóló 2015. Évi CCXXII. törvény.
Nytv.	A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény.
Szmtv.	2007. évi I. törvény a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról.
Harmtv.	2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló törvény
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
24/2016 BM rendelet	A bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016. (VI. 30.) BM rendelet.

Műszaki szakkifejezések rövidítései

ASN.1	Abstract Syntax Notation 1
CA	Certification Authority Kiadó
CAA	Certification Authority Authorization Bizalmi szolgáltató Felhatalmazás
IP	Internet Protocol
IT	Information Technology
BRG	Baseline Requirements Guidelines
CAB Forum	CA/Browser Forum
CP	Certificate Policy Hitelesítési Rend
CPS	Certification Practice Statement
CRL	Certificate Revocation List Tanúsítványvisszavonási lista
CSP	Certification Service Provider
EAL	Evaluation Assurance Level
EV	Extended Validation

EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
FQDN	Fully qualified domain name
gTLD	Generic top-level domain
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers
OCSP	Online Certificate Status Protocol Tanúsítványállapot-szolgáltatás
OID	Object Identifier Azonosító
OVC	Organizational Validation Certificate
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SAN SubjectAltName	Subject Alternative Name
SCD	Signature / Seal Creation Device Aláírás / Bélyegző Létrehozó eszköz (Nem minősített)
SSL	Secure Socket Layer
TLS	Transport Layer Security
TSP	Trust Service Provider Bizalmi Szolgáltató
QSCD Korábbi nevén SSCD	Qualified Signature / Seal Creation Device Minősített Aláírás / Bélyegző Létrehozó eszköz
UN	United Nations
IETF	Internet Engineering Task Force
QC	Qualified Certificate
URL	Uniform Resource Locator

Lásd még a dokumentum 9.15 pontjában foglaltakat.

2. Közzétételre vonatkozó felelősségek

2.1 Adattárak

Szolgáltató köteles az időbélyeg-szolgáltatásra vonatkozó különböző információk (szabályzatok, tanúsítványok, érvényességi információk, s az ezeket nyilvánosságra hozó szervezetek - ha eltér a szolgáltatótól) nyilvánosságra hozatalára; az elérésükhöz szükséges adatokat a Szolgáltatási Szabályzatában kell ismertetni.

2.2 Időbélyeg-szolgáltatásra és a szolgáltatói tanúsítványokra vonatkozó információk közzététele

A Szolgáltató köteles weboldalán (lásd 1.1.2) közzétenni az időbélyeg-szolgáltatás igénybevételéhez ügyfelek számára elengedhetetlen információkat valamint a szolgáltatás nyújtásához használt szolgáltatói tanúsítványokat a Kikötésekben előírt módon közzétenni. A jelen Szolgáltatási Rend alapján készült Szolgáltatási Szabályzatot az RFC 3647 ajánlás szerinti tartalommal és struktúrában kell közzétenni.

2.3 Közzététel időpontja és gyakorisága

Szolgáltatónak a szolgáltatáshoz kapcsolódó Kikötéseket és a dokumentumok újabb verzióit a hatályba lépésüket megelőzően közzé kell tennie. A korábbi verziókat az érvényességük végét követően is mindaddig közzé kell tennie, ameddig azok alapján élő szolgáltatási szerződések vannak.
A szolgáltatónak legalább évente felül kell vizsgálnia a Bizalmi Szolgáltatási Rendjét és szabályzatait, szükség esetén módosítva azokat (lásd 9.12).

2.4 Az információk elérésének szabályai

A szolgáltató szolgáltatásra vonatkozó publikus dokumentumainak, különösen a Kikötéseknek a Szolgáltató weboldalán (lásd 1.2.1) elérhetőknek kell lenniük olvasásra.

3 Azonosítás és hitelesítés

Szolgáltatónak megbízható adatforrások alapján ellenőriznie kell az Előfizető szolgáltatási szerződésbe kerülő adatait.

4 Életciklus követelmények

Jelen fejezet és alfejezetei a Szolgáltató által nyújtott időbélyeg-szolgáltatásra, a szolgáltatás igénylésére, a szolgáltatási szerződés megkötésére valamint a szerződés időtartama alatt végzendő szolgáltatói tevékenységekre és az Ügyfél által végezhető műveletekre vonatkozó specifikus előírásokat tartalmaz.

4.1 Szolgáltatás igénylése

A szolgáltatás igénybevételéhez Előfizetőnek Szolgáltatási szerződést kell kötnie Szolgáltatóval.
Szolgáltató a Szolgáltatási Szabályzatban, az ÁSZF-ben és a szolgáltatási szerződésben további feltételeket írhat elő a szolgáltatás igénybevételéhez.
A szolgáltatás igénylésének módját és elfogadásának feltételeit, a feldolgozás folyamatát valamint a szerződéskötés feltételeit Szolgáltatónak a Szolgáltatási szabályzatban kell ismertetnie.

4.2 A szolgáltatás nyújtása

A minősített időbélyeg-szolgáltatás nyújtása keretében a Szolgáltatónak fogadnia kell az Ügyfelektől érkező, jelen Szolgáltatási rend szerinti időbélyeg kéréseket, és azokat jelen Szolgáltatási rend szerinti időbélyeg válaszokkal kell kiszolgálnia a szolgáltatási szabályzatban és egyéb kikötésekben meghatározott módon.
A szolgáltatási szerződés megkötését követően Szolgáltatónak egyedi hozzáférést kell biztosítania Végfelhasználó számára az Időbélyeg-kiszolgálóhoz.
Szolgáltatónak a szerződéskötést követően tartós adathordozón át kell adnia az Ügyfélnek a jelen Szolgáltatási Rend alapján készült szolgáltatási szabályzatot és a szolgáltatási szerződést.
Az időbélyeg-kérések fogadásakor Szolgáltatónak a Szolgáltatási szabályzatban leírt módon azonosítania kell az időbélyeg-kérés küldőjét. A szolgáltatási szerződés életciklusában Szolgáltatónak joga van - a Kikötésekben meghatározott esetekben, kiváltképp a szerződésszegés esetét - a szolgáltatás korlátozásához vagy felfüggesztéséhez.

4.3 A szolgáltatási szerződés megszűnése

Nincs előírás.

4.4 Szolgáltatás elérhetősége és rendelkezésre állása

Szolgáltatónak Végfelhasználó azonosítását követően biztonságos HTTPS protokollon keresztül kell számára biztosítania a szolgáltatáshoz való hozzáférést a szolgáltatási szabályzatban leírt módon.
Szolgáltatónak biztosítania kell a szolgáltatás, valamint az annak keretében kibocsátott időbélyegek használatára vonatkozó kikötések és feltételek folyamatos elérhetőségét éves szinten legalább 99,9%-os rendelkezésre állás mellett, ahol az eseti szolgáltatáskiesések időtartama legfeljebb 3 óra.
Az időbélyeg-szolgáltatás korlátozás nélkül hozzáférhető az Ügyfelek számára, de túlzott használat esetén szolgáltatásvédelmi okokból egy határ átlépése esetén korlátozhatók a hozzáférések. A korlátozások feltételei közzétételre kerülnek a Szolgáltató weboldalán (lásd 1.1.2).

4.5 Javasolt eljárás az időbélyeg ellenőrzésére

Szolgáltatónak a szolgáltatási szabályzatban és/vagy a Szolgáltató weboldalán (lásd 1.1.2) tájékoztatást kell közreadnia az Érintett felek számára az általa kibocsátott időbélyegek ellenőrzéséhez
Az Időbélyegző ellenőrzése során ellenőrizni kell:

- az időbélyegen szereplő elektronikus aláírást és annak tanúsítványát
- hogy az időbélyegzett dokumentum, az időbélyegző és annak tanúsítvány összetartozik-e;
- hogy az időbélyeg pontossága, megbízhatósága, valamint a hozzá kapcsolódó szolgáltatói felelősségvállalás megfelel-e az adott célra.

Az időbélyegen szereplő aláírás vagy bélyeg tanúsítványának ellenőrzésekor Érintett feleknek a NETLOCK Bizalmi Szolgáltatási Szabályzat Minősített Tanúsítványszolgáltatásra, 4.9.6 Javasolt eljárás a tanúsítványállapot ellenőrzésére fejezete szerint javasolt eljárni.

5 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A Szolgáltatónak gondoskodnia kell arról, hogy az elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket, illetve az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazzon.

A Szolgáltatónak meg kell felelnie az alábbi követelményeknek:

- Rendszeresen elvégzett kockázatelemzéssel kell rendelkeznie (ennek részleteit lásd az 5.4.8-ban)
- Menedzsment által elfogadott, dokumentált, implementált és karbantartott információbiztonsági szabályozással kell rendelkeznie, beleértve a biztonsági kontrollok és műveleti eljárásokat a Szolgáltató létesítményei, rendszerei és információs eszközei számára, melyek a szolgáltatásnyújtást biztosítják. A Szolgáltató az információbiztonsági szabályozást minden érintett minden munkavállalójával.
- Szolgáltató felelősséget visel az információbiztonsági szabályozásában meghatározott eljárások betartásáért, akkor is, ha azokat nem szolgáltató saját személyzete végzi. Szolgáltatónak meg kell határoznia e közreműködők felelősségét, és biztosítania kell, hogy az előírt eljárásokat betartják.
- Az információbiztonsági szabályozást és vagyonnyilvántartást rendszeres időközönként, vagy ha jelentős változások történnek, felül kell vizsgálni, hogy biztosított legyen azok folyamatos alkalmazhatósága, megfelelősége és eredményessége. Minden változtatást, amely hatással van a biztonsági szintre, jóvá kell hagynia a Szolgáltató menedzsmentjének. A Szolgáltatói rendszerek konfigurációját rendszeresen ellenőrizni kell a biztonsági előírásokat sértő változások kiszűrése érdekében.

5.1 Fizikai óvintézkedések

A Szolgáltató gondoskodjon arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen, és a kritikus szolgáltatások eszközeinek fizikai kockázatát minimalizálják.

A Szolgáltató biztosítsa az értékek elvesztésének, sérülésének, és kompromittálódásának, valamint a működési tevékenységek megzavarásának elkerülését.

A Szolgáltató óvintézkedéseket valósítson meg az információ és az információ feldolgozó berendezések kompromittálódásának, illetve ellopásának elkerülése érdekében.

5.1.1 Telephely felépítése

A telephely kiépítése és a környezeti biztonság kezelése során szolgáltatónak figyelembe kell venni a tűz és vízvédelemre, a folyamatos áramellátásra, a légkondicionálásra, a fizikai behatolás megakadályozására, a biztonságos zónák kialakítására és a telekommunikációs hálózatok elérhetőségére és a sugárzás elleni védelemre vonatkozó ajánlásokat és előírásokat.

5.1.2 Fizikai hozzáférés

A Szolgáltató biztosítson egy egyértelműen meghatározott és fizikailag lehatárolt biztonsági területet a biztonságos működéséhez kritikus komponensei számára, amelyet a behatolás ellen fizikailag véd, ahova a bejutást ellenőrzi, az illetéktelen behatolást észleli és riasztani képes. Bármely más szervezettel, szervezeti egységgel megosztott rész e körleten kívül essen. Ugyanezen biztonsági területen belül más tevékenységek abban az esetben végezhetők, ha a területre belépési jogosultsággal rendelkezők azt el tudják végezni.

E kritikus szolgáltatások fizikai- és környezetbiztonsági programjai foglalkozzanak a fizikai hozzáférés szabályozásával, a természeti katasztrófa elleni védelemmel, a villámvédelem és tűzbiztonság tényezőivel, a támogató eszközök (ezen belül az áram és klíma berendezések) meghibásodásával, az építmény összeomlásával, vízvezeték szivárgással, talajvíz elleni védelemmel, lopás, betörés és behatolás elleni védelemmel, katasztrófa utáni helyreállítással.

Szolgáltató óvintézkedéseket valósítson meg

- a fizikai és környezetbiztonsági rendszererőforrások, illetve a működésük támogatására használt berendezések megvédése érdekében;
- annak megakadályozására, hogy az elektronikus aláírással kapcsolatos szolgáltatáshoz szükséges berendezés, információ, adathordozó vagy szoftver elvesszen, megsérüljön vagy jogosulatlanul elvigyék a helyszínről.

A Szolgáltató a kritikus szolgáltatásaival kapcsolatos eszközökhöz történő fizikai hozzáférést megfelelően felhatalmazott egyénekre korlátozza, s az eszközöket olyan környezetben működtesse, amely fizikailag megvédi a szolgáltatásokat attól, hogy a rendszerekhez, illetve adatokhoz történő jogosulatlan hozzáférésen keresztül kompromittálódjanak.

A biztonsági körletbe való belépéseket felügyelni kell, a nem jogosult személyek csak jogosult személyek felügyeletével tartózkodhatnak a körletben. A belépéseket és kilépéseket azok időpontjával és a tartózkodásának céljával együtt naplózni kell.

5.1.3 Áramellátás, légkondicionálás

A Szolgáltató szolgáltatási helyszíneire olyan szünetmentes áramellátást kell biztosítani, amely megfelelő teljesítménnyel rendelkezik a rendszerek áramellátásához, rövid idejű kimaradás esetén, és tartós áramszünet esetén saját áramtermelő berendezés segítségével biztosított a rendszerek további működése.

A szolgáltatási helyszínre bejutó levegő tisztaságát megfelelő szűrőrendszerrel kell biztosítani, amely kiszűri a levegőből a különféle szennyeződéseket, tovább biztosítja a szolgáltató munkatársai részére szükséges levegőt. A keringetett levegő nedvesség tartalmát és hőmérsékletét az informatikai rendszerek számára megfelelően kell beállítani.

A légkondicionáló rendszer teljesítménye olyan kell legyen, hogy képes legyen a szükséges hűtést biztosítani az IT rendszerek számára.

5.1.4 Beázás és elárasztódás veszélyeztetettsége

A Szolgáltató szolgáltatási helyszíneit védeni kell a beázástól és az elárasztódástól.

5.1.5 Tűzmegelőzés és tűzvédelem

A Szolgáltató szolgáltatási helyszíneit védeni kell a tűztől.

Az aktuális tűzvédelmi szabályzásoknak megfelelő tűz és füstérzékelőket, kézi és automata oltó berendezéseket kell felszerelni, jelezni kell a kézi oltó berendezések helyét, a menekülési útvonalat.

5.1.6 Adathordozók kezelése

A Szolgáltató az adathordozó eszközöket biztonságosan kezelje a sérülés, ellopás és jogosulatlan hozzáférés és az avulás elleni védelem érdekében. A Szolgáltató az összes adathordozó eszközt biztonságosan kezelje az adat-minősítési rendszer követelményeinek megfelelően. A média avulását és sérülését meg kell akadályozni az adatok teljes megőrzési idejében.

A Szolgáltató az érzékeny adatokat tartalmazó adathordozó eszköztől biztonságosan váljon meg, amennyiben azokra már nincs szükség. A selejtezett eszközök tartalmát - széles körben elfogadott módszerek alapján – véglegesen törölni kell, vagy az eszközt egyéb módon helyreállíthatatlanul tönkre kell tenni.

A Szolgáltatónak a kritikus adatokról több mentési példánnyal kell rendelkeznie, és egy példányt a szolgáltatói helyszíntől eltérő olyan külső helyszínen kell tárolni, melyben a mentések védelmének szintje azonos a szolgáltatási helyszínével.

5.1.7 Hulladékelhelyezés

Informatikai eszközeinek selejtezése esetén a szolgáltatónak biztonságosan és helyreállíthatatlanul törölnie kell az azon tárolt adatokat, vagy ha ez nem lehetséges legalább az ilyen elemet hordozó alkatrészt fizikai tönkretétellel megsemmisíti, ami annak olvashatóságát megakadályozza.

Iratok selejtezése esetén a személyes adatot tartalmazó iratokat megfelelő eljárással olvashatatlanná kell tenni.

Szolgáltatónak követni kell a hulladékról szóló 2012. évi CLXXXV. törvényt és a hivatkozott kormányrendeletet az elektronikai hulladékok megsemmisítése tekintetében.

5.1.8 Mentés külső helyszínen

A Szolgáltatónak az üzemmenet folytonossága és az adatvesztés elkerülése érdekében

mentéseket kell végeznie, és biztosítania kell az informatikai rendszer egészének szükség esetén való helyreállíthatóságát. A mentéseket védeni kell a jogosulatlan módosítástól, törléstől, megsemmisüléstől és a jogosulatlan hozzáféréstől. A rendkívüli helyzetekre való felkészülés magában foglalja a kidolgozott tervek adott esetekre történő alkalmazását és tesztelését is.

A megőrzendő adatok biztonságos tárolását a szolgáltató elvégezheti csak írható médiával, távoli helyen tárolt mentéssel, vagy több tárolási helyen történő távoli párhuzamos tárolással.

5.2 Eljárásrendi biztonsági intézkedések

Szolgáltatónak gondoskodnia kell rendszerei biztonságos, szabályszerű, a meghibásodás minimális kockázata melletti üzemeltetéséről. Ennek érdekében elegendő számú és megfelelő képzettséggel, műszaki tudással, tapasztalattal rendelkező személyzetet kell alkalmaznia.

A Szolgáltató a jogszabályoknak és szabályzatainak megfelelő és naprakész belső irányítási és ellenőrzési eljárásrendet és kapcsolódó felelősségi rendszert kell működtessen. A rendszer megfelelő működését a független rendszervizsgáló ellenőrzési tevékenységének kell biztosítani.

A Szolgáltatónak külső, független rendszervizsgáló által folyamatosan ellenőrzött minőségirányítási és információbiztonsági irányítási rendszerrel kell rendelkeznie.

A Szolgáltatónak a minősített szolgáltatás nyújtása során létrejövő és kezelt adatot a jogszabályok és a szolgáltatási szabályzatban meghatározott kockázatelemzés alapján biztonsági osztályba kell sorolnia, és gondoskodnia kell azok megfelelő nyilvántartásáról, ellenőrzéséről, védelméről, valamint az ehhez szükséges felelősségi rendszer működtetéséről.

5.2.1 Bizalmi munkakörök

A Szolgáltatónál bizalmi munkakört csak olyan személy tölthet be, akinek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét, szakértelmét a minősített szolgáltató szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

Az informatikai rendszerért általánosan felelős munkakört olyan személynek kell betöltenie, aki szakirányú felsőfokú végzettséggel[3] és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik.

A minősített szolgáltató a bizalmi munkakört betöltő személyt munkaviszonyban köteles foglalkoztatni, és a bizalmi munkakört betöltő személynek függetlennek kell lennie minden olyan érdektől, amely hátrányosan érintheti a minősített szolgáltatás megbízhatóságát és biztonságát. A minősített szolgáltatónak gondoskodnia kell arról, hogy a minősített szolgáltatások nyújtásával kapcsolatban álló személy a szükséges és megfelelően naprakész tudással és tapasztalattal rendelkezzen. A minősített szolgáltató valamennyi bizalmi munkakör betöltését köteles biztosítani, és a bizalmi munkaköröket nevesítenie kell.

Bizalmi munkaköröknek kell tekinteni a következőket:

[3] Szakirányú felsőfokú végzettség a matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség.

- Biztonsági tisztviselő: A szolgáltatás biztonságáért általánosan felelős személy.
- Rendszeradminisztrátor: A szolgáltató informatikai rendszer telepítését, konfigurálását, karbantartását végző személy.
- Rendszerüzemeltető: A szolgáltató informatikai rendszerének folyamatos üzemeltetését, mentését és helyreállítását végző személy.
- Független rendszervizsgáló: A szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy

Bizalmi munkakört kizárólag a Szolgáltatóval munkaviszonyban álló munkatárs tölthet be, a Szolgáltató felső vezetésének formális kinevezését követően. Bizalmi munkakör megbízási szerződés alapján nem tölthető be.

A bizalmi munkakörökről naprakész nyilvántartást kell vezetni, változás esetén a változás tényét haladéktalanul be kell jelenteni a Bizalmi Felügyeletnek.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszám

Szolgáltatónak a szolgáltatási szabályzatban kell előírnia, hogy az időbélyeg-szolgáltatás kapcsán végzendő szolgáltatói műveletek közül melyek végezhetők kizárólag két bizalmi munkakört betöltő munkatárs együttes fizikai jelenlétével és/vagy egy fizikailag védett környezetben és/vagy más személyek jelenlétét kizárva.

5.2.3 Az egyes szerepkörökhöz tartozó azonosítás és hitelesítés

Szolgáltató köteles az informatikai rendszerének minden felhasználóját és az adminisztratív folyamatok minden szereplőjét személy szerint azonosítani, kivéve a nyilvános adatszolgáltatásához kizárólag olvasási jogosultsággal rendelkező felhasználókat.

Szolgáltató informatikai rendszereihez csak az arra felhatalmazott személyek férhetnek hozzá. A szolgáltatónak adminisztrálnia kell a rendszeradminisztrátorok, rendszerüzemeltetők és Független rendszervizsgálók rendszerhozzáférését, beleértve a felhasználói fiók kezelését, alkalmi módosítását és adott esetben a hozzáférés megszüntetését.

Az egyes alkalmazásokhoz való hozzáféréseknek szolgáltató szabályozása szerint korlátozhatónak kell lennie. A rendszernek el kell tudnia különíteni az egyes bizalmi munkaköröket, így különösen a rendszeradminisztrátori és rendszerüzemeltető hozzáféréseket.

A személyzetet azonosítani és hitelesíteni kell a szolgáltatások szempontjából kritikus alkalmazások használata előtt, s tevékenységükkel kapcsolatban elszámoltathatónak kell lenniük.

5.2.4 Egyes szerepkörök összeférhetetlensége

A szolgáltatói eszközökben, rendszerekben végrehajtott azonosítatlan vagy nem szándékolt módosítások illetve más visszaélések lehetőségének csökkentése érdekében a Szolgáltatónak az egymást kizáró feladatokat és felelősségi területeket el kell különíteni.

A feladatkörök elhatárolása végett

- a biztonsági tisztviselő nem láthatja el a független rendszervizsgáló, a

Rendszeradminisztrátor és az informatikai rendszerért általánosan felelős vezető feladatait, valamint
- a független rendszervizsgáló nem láthatja el a Regisztrációs felelős, a Rendszeradminisztrátor és az informatikai rendszerért általánosan felelős vezető feladatait;
- az informatikai rendszerért általánosan felelős vezető nem láthatja el a biztonsági tisztviselő és a független rendszervizsgáló feladatkörét.

5.3 Személyzeti biztonsági intézkedések

A Szolgáltató gondoskodjon arról, hogy alkalmazottai és szerződéses partnerei támogassák a szolgáltatások megbízhatóságát. A Szolgáltató bizalmi munkakörben foglalkoztatott személyzetének minden olyan összeférhetetlenségtől mentesnek kell lennie, amely a szolgáltatások nyújtásában végzett tevékenységének pártatlanságát sértheti

A személyzetnek az informatikai biztonsági eljárásokkal összhangban kell végrehajtani az adminisztrációs és menedzsment eljárásokat.

Az információbiztonsági szabályzatban azonosított biztonsági munkaköröket és felelősségeket munkaköri leírásokban vagy más az érintett felek számára elérhető dokumentációban dokumentálni kell. A bizalmi munkaköröket világosan meg kell határozni, be kell tölteni, és a megbízást el kell fogadnia a menedzsmentnek és az érintett személynek egyaránt.

A személyzetnek (beleértve az állandóan és ideiglenesen foglalkoztatottakat egyaránt) olyan munkaköri leírásokkal kell rendelkezni, amelyek a feladatok szétválasztása és legkevesebb jogosultság elvéből indulnak ki, s a pozíció bizalmas jellegének meghatározása a feladatok, a hozzáférési szintek, a háttér szűrés és az alkalmazott képzése és tudatossága alapján történik.

5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények

A Szolgáltató valamennyi munkatársának rendelkeznie kell a munkaköre ellátásához szükséges végzettséggel, gyakorlattal, megbízhatósággal és szakmai ismeretekkel, tapasztalattal. A Szolgáltató bizalmi munkakörben csak büntetlen előélettel rendelkező alkalmazottakat foglalkoztathat, melyet a felvételi eljárás során 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni.

A minősített szolgáltatónál bizalmi munkakört csak olyan személy tölthet be, akinek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét, szakértelmét a minősített szolgáltató szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

Az informatikai rendszerért általánosan felelős munkakört olyan személynek kell betöltenie, aki a 24/2016 BM rendelet által elfogadott szakirányú felsőfokú végzettséggel és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik.

Szolgáltató a bizalmi munkatársakat munkaviszonyban köteles foglalkoztatni. Szolgáltatónak a bizalmi munkakörre jelölt személy foglalkoztatásának megkezdése előtt meg kell győződnie arról jelölt független minden olyan érdektől, amely hátrányosan érintheti a minősített

szolgáltatás megbízhatóságát és biztonságát.

Szolgáltatónak gondoskodnia kell arról, hogy a minősített szolgáltatások nyújtásával kapcsolatban álló személy a szükséges és megfelelően naprakész tudással és tapasztalattal rendelkezzen (lásd 5.3.3 és 5.3.4).

Szolgáltató köteles biztosítani valamennyi bizalmi munkakör betöltését, és a bizalmi munkaköröket a szolgáltatási szabályzatban nevesítenie kell.

A szolgáltató menedzsmentjének megfelelő tapasztalattal kell bírnia a szolgáltató által nyújtott bizalmi szolgáltatások területén, valamint informatikai biztonsági és kockázatkezelési területeken, valamint a biztonságért felelős menedzsereknek a biztonsági eljárások területén, annak érdekében, hogy menedzsment feladataikat elláthassák.

A Szolgáltató köteles olyan munkatársakat és adott esetben olyan alvállalkozókat alkalmazni, akik megbízhatóak, rendelkeznek a szükséges szakértelemmel, tapasztalattal és képesítésekkel, valamint megfelelő képzésben részesültek a biztonságra és a személyes adatok védelmére vonatkozó szabályokkal kapcsolatban, továbbá köteles olyan igazgatási és ügyvezetési eljárásokat alkalmazni, amelyek megfelelnek az európai és nemzetközi szabványoknak.

5.3.2 Ellenőrzési eljárások

A Szolgáltatónak a bizalmi munkakörben foglalkoztatandó személyek esetében (a szerződéses viszonytól függetlenül) meg kell győződnie e személyek személyazonosságáról fizikai jelenlétük során vagy fényképes személyazonosító okmányaik ellenőrzésével. Valamint meg kell győződniük e személyek megbízhatóságáról, ami magában foglalja a korábbi munkahelyekre, releváns végzettségekre és szakmai referenciákra vonatkozó információk ellenőrzését. Az ellenőrzések lefolytatását megelőzően nem kaphatnak hozzáférést a szolgáltató rendszereihez.

5.3.3 Képzési követelmények

A szolgáltatónak meg kell bizonyosodni arról, hogy a bizalmi munkakörben dolgozó személyek rendelkeznek a feladataik ellátásához szükséges tudással. Ennek érdekében vizsgát kell tenniük a szükséges ismeretek birtoklását igazolandó. A Szolgáltató bizalmi szolgáltatást nyújtó rendszereihez hozzáférési jogosultságot csak a sikeres vizsgát tevő személyek kaphatnak. A vizsga megtörténtét dokumentálni kell. A szolgáltatónak a vizsgát megelőzően az érintett személyek számára szükség szerinti mértékben támogatni kell a hiányzó ismeretek megszerzését a feladatuk ellátásához szükséges mértékben. A vizsgának és a képzésnek a következőket kell felölelnie:

- PKI alapismeretek;
- hitelesítés és ellenőrzési szabályok és eljárások;
- Biztonsági és adatvédelmi szabályok;
- általános fenyegetések az információhitelesítési eljárásokra (beleértve az adathalász és egyéb social engineering taktikákat);
- jelen Bizalmi Szolgáltatási Rend, a Szolgáltatási Szabályzat és egyéb szabályzatok előírásai;
- egyes tevékenységük jogi következményei;
- Szolgáltató informatikai rendszerének sajátosságai és kezelésének módja;

5.3.4 Továbbképzési gyakoriságok és követelmények

A Szolgáltatónak gondoskodnia kell róla, hogy a bizalmi munkakört ellátó személyek folyamatosan rendelkezzenek a feladataik ellátásához szükséges tudással, így szükség esetén továbbképzést, vagy ismétlő jellegű képzést kell tartania. Így továbbképzést kell tartania, amennyiben a szabályzataiban vagy informatikai rendszerében olyan változás áll be, ami érinti e munkakörök tevékenységét. Legalább 12 havonta tájékoztatni kell a személyzetet - minden munkatársat a munkakörének megfelelő mértékben - az előző 12 hónapban ismertté vált esetleges új fenyegetettségekről és az aktuális biztonsági eljárásokról.

A továbbképzést megfelelően dokumentálni kell, amelyből utólag is megállapítható a továbbképzés tematikája és a résztvevők személye.

5.3.5 Munkabeosztás körforgásának sorrendje és gyakorisága

Nincs előírás.

5.3.6 Jogosulatlan tevékenységek büntető következményei

A Szolgáltatónak megfelelő fegyelmi szankciókat kell alkalmazni szolgáltatói rendszerének nem engedélyezett használata vagy a szolgáltatás nyújtása közben elkövetett hibák, mulasztások, károkozások esetére az azt okozó alkalmazottak vagy közreműködő természetes és jogi személyek esetében. A lehetséges szankciókról a velük kötött szerződésben rendelkezni kell.

5.3.7 Szerződéses közreműködőkre vonatkozó követelmények

A Szolgáltató által szerződéses viszonyban közreműködő személyekre ugyanúgy vonatkoznak a szabályzatok elvárásai, mint az alkalmazottaira.

5.3.8 A személyzet számára biztosított dokumentációk

A Szolgáltatónak folyamatosan biztosítania kell a szolgáltatásnyújtásban közreműködő személyek részére a szerepkörük ellátásához szükséges aktuális szabályzatok és dokumentációk elérhetőségét.

5.4 Naplózási eljárások

A minősített szolgáltatónak minden, az informatikai rendszerével és a minősített szolgáltatás nyújtásával kapcsolatos eseményt, illetve az általa vagy számára kibocsátott adatokra vonatkozó összes lényeges információt - az üzemmenet folytonossága, az adatvesztés elkerülése, bizonyítékok bírósági eljárások során történő bemutatása, valamint az informatikai biztonság biztosítása érdekében - folyamatosan naplóznia kell. A naplózott adatállománynak a minősített szolgáltatás nyújtásának teljes folyamatát át kell fognia, és alkalmasnak kell lennie a minősített szolgáltatással kapcsolatos minden esemény rekonstruálására a valós helyzetek megítéléséhez szükséges mértékben.

A naplózott adatállománynak a naplózott esemény bekövetkeztének naptári napját és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat és az eseményt előidéző felhasználó vagy más személy nevét kell tartalmaznia.

A naplózott adatállomány minden bejegyzését védeni kell a módosítástól és a jogosulatlan hozzáféréstől. A naplót úgy kell kezelni, hogy kizárható legyen a napló megsemmisítése, a napló bejegyzéseinek törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása, s hogy e védelmek a szolgáltató tevékenységeinek beszüntetését követő időszakra is kiterjedjenek. A minősített szolgáltató a naplóról rendszeres mentést készít.

A minősített szolgáltatónak gondoskodnia kell a naplóadatok folyamatos értékeléséről és ellenőrzéséről.

Szolgáltatónak dokumentálni kell a naplózott információk elérésének módját és megőrzési idejét.

Időbélyegző szolgáltatás kapcsán naplózni kell a következő eseményeket:

- Az időbélyegző kiszolgáló kulcsával és tanúsítványával kapcsolatos életciklus események
- Minden jellegű óraszinkron esemény, beleértve a szinkronizáció elvesztésének detektálását is.

A Szolgáltatónak rögzíteni és egy meghatározott ideig folyamatosan hozzáférhetővé kell tenni - a tevékenységének megszűnése utáni időszakban is - minden lényeges információt beleértve a kiadott és fogadott adatokat, különösen a bírósági eljárásokban bizonyítékként való felhasználás érdekében, valamint a szolgáltatásfolyamatosság biztosítása céljából és a megfelelőségértékelés számára.
A naplóbejegyzések mellett el kell tárolni

- az bejegyzés (és ha eltér az esemény) dátumát és időpontját;
- az esemény típusát;
- az esemény-végrehajtás sikerességét illetve sikertelenségét;
- a felhasználó vagy rendszer azonosítóját, aki/amely az eseményt kiváltotta.

Amennyiben naplózó és naplóelemző rendszer működésében komoly rendellenesség lép fel, a Szolgáltató működését fel kell függeszteni az üzemzavar elhárításáig.

Az események mellett rögzített időinformációt legalább naponta szinkronizálni kell hiteles időforrással.

5.4.1 A tárolt események típusai

Az automatikusan és manuálisan rögzített naplóállományokban az alábbi eseményeket el kell tárolni:

1. Biztonsági események
    a. Biztonsági profil változások
    b. Rendszer indítása és leállítása
    c. Tűzfal és router tevékenységek
    d. Szolgáltatói rendszer hozzáférési kísérletek módja és eredménye (sikeres és sikertelen)
    e. Szolgáltatói létesítménybe történő belépések és kilépések
2. Szolgáltatói rendszer beállításai
    a. Rendszer telepítése
    b. Rendszerkonfiguráció változásai (pl. frissítések, foltozások, beállítások)

    c. Rendszer vagy rendszeradatok mentése és visszaállítása
3. Pontos időt érintő események
    a. Óraszinkronizációs események
    b. Előírt időpontossági küszöb túllépése
4. Naplózási események
    a. Naplózó rendszer leállítása, újraindítása;
    b. Naplózási beállítás módosítása
    c. Naplózási adatok archiválása-törlése;
5. Felhasználómenedzsment műveletek (Szolgáltatói rendszerek tekintetében)
    a. Felhasználók felvétele, törlése
    b. Szerepkörök vagy jogosultságok kiosztása, visszavonása
    c. Státuszváltozások (pl. zárolás, tiltás, engedélyezés)
    d. Előírt azonosítási módszer beállításai
    e. Hitelesítési adat (pl. jelszó) cseréje
6. Rendellenes vagy veszélyt jelentő események
    a. Rendszerösszeomlás és a hardver hibák;
    b. Bármilyen szoftverművelet hibája;
    c. Szoftverintegritás hiba;
    d. Hálózati támadási kísérletek;
    e. Elektromos hálózati üzemzavar;
    f. Szünetmentes tápegység hiba;
    g. Kommunikációs üzemzavar.

Az ügyfelek szolgáltatásigénylései kapcsán az alábbi információk rögzítése szükséges:

- A műveletek dátuma és pontos ideje;
- Az aláírt szolgáltatási szerződés vagy másolata és tárolási helye
- Az ügyfél által végzett bármilyen választás a szolgáltatás tekintetében (pl. szolgáltatási szerződésben)
- Az Ügyféligényt feldolgozó személy azonosítója

5.4.2 A naplófájl feldolgozásának gyakorisága

A Szolgáltatónak biztosítania kell a keletkezett naplóállományok rendszeres kiértékelését. A naplóállományokban rögzített bejegyzéseket a keletkezésüktől számított legkésőbb 1 héten belül ki kell értékelni a megfelelő szakértelemmel és jogosultságokkal rendelkező Független rendszervizsgálónak. A kiértékeléshez szoftvereszközök is igénybe vehetők.

A kiértékelés során meg kell győződni a vizsgált naplóállományok hitelességéről és sértetlenségéről.

A kiértékelés során elemezni kell

- a rendszerek által generált hibaüzeneteket,
- a forgalmi adatokban bekövetkezett jelentős változásokat,
- a szokványostól eltérő bármilyen rendkívüli mintákat,
- gyanús aktivitásokat.

A kiértékelés tényét, eredményeit és az esetlegesen feltárt problémák és kockázatok elhárítása érdekében meghozott intézkedéseket dokumentálni kell.

Az automatikus kiértékelő eljárásoknak riasztani kell a személyzetet a biztonságilag kritikusnak tűnő események észlelése esetén.

5.4.3 A naplófájl megőrzési időtartama

A naplóállományokban rögzített információkat meg kell őrizni legalább 10 évig (a Szolgáltatói rendszerben vagy archivált formában).

A Független rendszervizsgáló számára bármikor elérhetővé kell tenni a naplózott információkat.

5.4.4 A naplófájl védelme

Gondoskodni kell arról, hogy a naplóállományok, illetve a benne rögzített információk ne legyenek egyszerűen törölhetők vagy megsemmisíthetők. A rögzített információk bizalmasságát és integritását (beleértve a még nem és már archivált eseményeket is) fenn kell tartani a megőrzési idő végéig. A naplóállományokhoz csak az arra jogosultak – elsősorban a Független rendszervizsgálók – férhessenek hozzá. Jogi eljárás esetén az érintett információkat elérhetővé kell tenni az eljárásban érintett és erre feljogosított személyek számára.

5.4.5 A naplófájl mentési eljárásai

A naplóállományokat 2 példányban, fizikailag elkülönülő helyeken kell tárolni. Amennyiben a naplóbejegyzés egy helyen keletkezik, akkor legkésőbb 24 órán belül gondoskodni kell arról, hogy egy másik helyszínen is létrejöjjön róla másolat. Lásd az *5.1.6 Adathordozók kezelése* és *5.1.8. Mentés külső helyszínen* fejezeteit.

5.4.6 A naplózás adatgyűjtési rendszere

Nincs előírás.

5.4.7 Az eseményeket kiváltó Ügyfelek értesítése

Nincs előírás.

5.4.8 Sebezhetőség felmérése

A Szolgáltatónak legalább negyedévente sebezhetőség felmérést kell végeznie, amely segítségével

- Azonosítja az előrelátható belső és külső fenyegetettségeket, amelyek lehetővé tehetik a szolgáltatás jogosulatlan elérését vagy a tárolt adatok nyilvánosságra hozatalát, megváltoztatását megsemmisítését vagy más visszaélést.
- Feltérképezi e fenyegetettségek bekövetkezésének valószínűségét és a bekövetkezés esetén várható kárt is.
- Értékeli a feltárt fenyegetettségek elhárítására alkalmazott folyamatok, védelmi intézkedések és informatikai rendszerek megfelelőségét.

5.5 Adatok archiválása

A Szolgáltató a szolgáltatással kapcsolatosan rendelkezésére álló adatokat - ide értve a személyes adatokat is köteles megőrizni (időtartamot lásd az 5.5.2 fejezetben).

A Szolgáltatónak az archivált adatállomány minden bejegyzését védenie kell a jogosulatlan módosítástól, törléstől, megsemmisüléstől és jogosulatlan hozzáféréstől. Az elektronikus formában tárolt archivált adatállományt legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel, és időbélyegzővel kell ellássa. A minősített szolgáltató köteles biztosítani, hogy mindaddig, amíg az adatokat őrzi, azok hitelesek, az arra jogosult személyek számára hozzáférhetők és értelmezhetők legyenek.

5.5.1 Az archiválandó adatok típusa

A Szolgáltatónak az időbélyeg-szolgáltatással kapcsolatosan rendelkezésére álló információkat és az ahhoz kapcsolódó személyes adatokat meg kell őriznie. Így például:

- a szolgáltatás igénylése során bekért és beszerzett információkat és dokumentációt;
- a jelen Bizalmi Szolgáltatási rend szerint naplózott információkat (5.4 Naplózási eljárások).

5.5.2 Archiválási időtartam

A Szolgáltató a naplózott adatokat a keletkezésüktől, a szolgáltatási szabályzatot és annak módosításait pedig hatályon kívül helyezésétől számított 10 évig köteles megőrizni, vagy megőrzéséről gondoskodni.

5.5.3 Az archívum védelme

Az 5.4.4. A naplófájl védelme fejezetben írtak szerint kell eljárni.

5.5.4 Az archívum mentési folyamatai

Az 5.4.5. A naplófájl mentési eljárásai fejezetben írtak szerint kell eljárni.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

A Szolgáltató az archiválandó adatokat időadattal, vagy időbélyeggel látja el.

5.5.6 Az archívum gyűjtési rendszere

Nincs előírás.

5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

Nincs előírás.

5.6 Kulcscsere

Szolgáltatónak le kell cserélnie kulcsát amennyiben valamely saját szolgáltatói tanúsítványa lejár, illetve, amennyiben alkalmazott kulcsai elavulnak, továbbá saját belátása szerint egyéb esetben is dönthet kulcscsere mellett.
Az új kulccsal kiállított új tanúsítvány esetében annak profilját és adatait az aktuális előírásokhoz és legjobb gyakorlathoz kell igazítani.

5.7 Katasztrófaelhárítás és helyreállítás

Szolgáltatónak megfelelő technikai és szervezeti intézkedéseket kell végrehajtani az általuk nyújtott bizalmi szolgáltatások biztonságát fenyegető kockázatok kezelése érdekében. Ezen intézkedésekkel – figyelembe véve a legújabb technológiai fejleményeket – biztosítani kell, hogy a biztonsági szint arányos legyen a kockázat mértékével. Intézkedéseket kell végrehajtani különösen a biztonsági események megelőzése és azok hatásának minimálisra csökkentése, valamint az érdekeltek bármely esemény káros hatásairól való tájékoztatása érdekében.

Szolgáltatónak indokolatlan késedelem nélkül, de minden esetben az esetről való értesüléstől számított 48 órán belül értesíteni kell a felügyeleti szervet és adott esetben más érintett szerveket, például az információbiztonságért felelős nemzeti szervet vagy az adatvédelmi hatóságot a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről, amennyiben az jelentős hatást gyakorol a bizalmi szolgáltatásra vagy az annak keretében tárolt személyes adatokra.

Amennyiben a biztonság megsértése vagy az adatok sértetlenségének megszűnése vélhetőleg hátrányosan érintheti azt a természetes személyt vagy szervezetet, aki bizalmi szolgáltatást vett igénybe, a Szolgáltató a természetes személyt és szervezetet is indokolatlan késedelem nélkül értesíti a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről.

5.7.1 Incidens- és kompromittálódáskezelési eljárások

Az informatikai rendszerekbe való belépésekre, azok felhasználóira és a szolgáltatásigénylésekre vonatkozó rendszertevékenységeket a Szolgáltatónak folyamatosan ellenőriznie kell, az alábbi szempontokat figyelembe véve:

1. A tevékenységek ellenőrzésénél figyelemmel kell lenni a begyűjtött és elemzett adatok érzékenyégére.
2. A potenciális biztonsági sérülésre utaló rendellenes rendszertevékenységet (beleértve a szolgáltatói hálózatba való behatolást is), a Szolgáltatónak azonosítania és jelentenie kell.
3. A szolgáltatói informatikai rendszereknek az alábbi eseményeket kell ellenőriznie:
    a. a naplózási funkciók indítását és leállítását;
    b. a bizalmi szolgáltatások rendelkezésre állását és működőképességét.
4. A Szolgáltatónak rövid időn belül és összehangoltan kell eljárnia a káreseményre való minél gyorsabb reagálás és a biztonsági sérülés hatásainak korlátozása érdekében. A Szolgáltatónak meg kell jelölnie azon riasztásokat és potenciálisan kritikus eseményeket, melyeket a bizalmi személyzetnek nyomon kell követnie és melyekről a belső szabályzatok szerint jelentést kell tennie.
5. Szolgáltató eljárásokat határoz meg az érintett felek értesítése érdekében a biztonságát vagy integritását sértő azon eseményekről, melyek jelentős hatással vannak a bizalmi szolgáltatásra vagy az abban kezelt személyes adatokra.
6. Szolgáltató egy korábban nem ismert kritikus sebezhetőséget a felfedezése után 48 órán belül kezel. Ha ez nem lehetséges, akkor létrehoz és életbe léptet egy tervet, amivel a kritikus sebezhetőség veszélyét enyhítheti, vagy tényszerűen dokumentálja, hogy a biztonsági rés nem igényel ilyen lépéseket.

7. Incidensjelentési és reagálási eljárásokat léptet életbe, melyekkel a biztonsági incidensek és zavarok okozta károk minimálisra csökkenthetők.

A Szolgáltatónak rendelkeznie kell Incidenskezelési és Katasztrófa-helyreállítási tervvel.

A Szolgáltató az üzletfolytonossági és katasztrófa-helyreállítási tervében dokumentálja azokat az eljárásokat, amivel értesíti és - lehetőség szerint - megvédi az Ügyfeleket és az érintett feleket katasztrófa, biztonsági kompromittálódás vagy üzleti kudarc esetén. Szolgáltató nem köteles nyilvánosságra hozni üzletfolytonossági és katasztrófa-helyreállítási tervét, de elérhetővé teszik őket a Független rendszervizsgálók kérésre. Szolgáltatónak évente tesztelni, felülvizsgálni, és frissítenie kell ezeket az eljárásokat.

Az üzletfolytonossági tervnek tartalmaznia kell:

1. A tervben foglalt intézkedések aktiválásának feltételei,
2. Vészhelyzeti eljárások,
3. Üzemszüneti eljárások,
4. Újraindulási eljárások,
5. A terv karbantartási ütemezése,
6. Tudatosító és oktatási követelményeknek,
7. Egyéni felelősségek,
8. Helyreállítási idő célkitűzés (RTO),
9. A készenléti tervek rendszeres vizsgálata,
10. Szolgáltató terve az üzleti tevékenységének fenntartására vagy helyreállítására kritikus üzleti folyamatainak sérülése vagy megszakadása esetén,
11. A kritikus kriptográfiai eszközök (kulcsok, kulcstároló eszközök, aktiváló kódok) eltérő helyen való tárolása;
12. Elfogadható kiesési és helyreállítási idő
13. A fontos üzleti információkról és szoftverekről történő biztonsági másolatotok készítésének gyakorisága,
14. A helyreállító létesítmények távolsága az elsődleges üzletviteli helyszíntől,
15. A berendezések biztosítására szolgáló eljárások katasztrófa után és a helyreállítás előtt az eredeti, vagy egy távoli helyszínen.

5.7.2 IT erőforrások, szoftverek és/vagy adatok meghibásodása

A Szolgáltató informatikai rendszereit megbízható hardver és szoftver komponensekből kell felépíteni.

A kritikus funkciókat redundáns rendszerelemek alkalmazásával kell megvalósítani úgy, hogy azok egy elem meghibásodása esetén is képesek legyenek a további működésre.

A Szolgáltató olyan gyakorisággal készítsen teljes rendszermentést, amely biztosítja, hogy abból katasztrófa esetén a teljes szolgáltatás helyreállítható legyen.

A Szolgáltató üzletfolytonossági terve tartalmazzon előírásokat a kritikus rendszerelemek meghibásodása esetén végrehajtandó feladatokra.

A Szolgáltató a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leghamarabb indítsa újra a szolgáltatásait.

Adatmentés és helyreállítás

- Szolgáltató működésének helyreállításához szükséges adatokat menteni szükséges,

és biztonságos, lehetőleg távoli helyen kell tárolni, ami alkalmas arra, hogy lehetővé tegye a Szolgáltató működésének helyreállítását incidens vagy katasztrófa esetén.
- A fontos üzleti információkról és szoftverekről rendszeresen biztonsági másolatotok kell készíteni. Megfelelő biztonsági mentési eszközöket kell biztosítani annak érdekében, hogy minden lényeges információt és szoftvert helyre lehessen állítani katasztrófa vagy médiasérülés után. A mentési rendszert rendszeresen tesztelni kell az üzletfolytonossági tervnek való megfelelés biztosítása érdekében.
- A biztonsági mentési és helyreállítási funkciókat 5.3 pontban meghatározott, releváns megbízható szerepkörrel rendelkező személyzetnek kell elvégezni.
- Amennyiben az előírások kettős kontrollt követlenek meg az adat kezeléséhez, akkor ezek helyreállításához is kettős kontrollt kell alkalmazni.

5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás

A szolgáltatói kulcs kompromittálódása esetén a Szolgáltatónak legalább:
- Tájékoztatnia kell az Ügyfeleit, Szolgáltatói partnereit, az Érintett feleket és a bizalmi felügyeletet.
- Jeleznie kell, hogy az érintett szolgáltatói kulccsal kibocsátott tanúsítványok és tanúsítványállapot-információ már nem érvényesek; és
- Vissza kell vonni az érintett Szolgáltatói tanúsítványt.

Amennyiben bármelyik algoritmus (vagy a kapcsolódó paraméterek) - amiket a Szolgáltató vagy a Végfelhasználók alkalmaznak - nem felel meg az elvárásoknak a fennmaradó tervezett felhasználási időtartamra, akkor a Szolgáltató köteles:
- Tájékoztatnia kell az Ügyfeleit, Szolgáltatói partnereit, az Érintett feleket és a bizalmi felügyeletet; és
- Vissza kell vonnia mindegyik érintett tanúsítványt.

5.7.4 A működés folytonosságának fenntartása katasztrófaesemény után

A szolgáltatónak rendelkeznie kell üzletfolytonossági tervvel, amit katasztrófa esetén életbe léptethet. Katasztrófa bekövetkezte estén Szolgáltató normál működése a tervben foglalt időszakon belül helyreállítandó, s egyúttal gondoskodni kell az ismételten bekövetkezhető hibák megelőzéséről is.

Katasztrófa esetén a normál üzletmenet a lehető leghamarabb helyreállítandó.

A Szolgáltatónak a szolgáltatás folytonosságának biztosítása érdekében a rendkívüli üzemeltetési helyzetek esetére olyan eljárással kell rendelkeznie, amely lehetővé teszi a minősített szolgáltatás mielőbbi helyreállítását.

Amennyiben a rendkívüli üzemeltetési helyzet meghaladja az eseti szolgáltatáskiesésre a 24/2016 BM rendelet 45.§-ban meghatározott legfeljebb 3 órás időtartamot, a minősített szolgáltató köteles a bizalmi felügyeletet haladéktalanul értesíteni a rendkívüli üzemeltetési helyzettel kapcsolatos alábbi információkról is:
- a rendkívüli üzemeltetési helyzet kezdetének, és ha eltér, észlelésének időpontja és a rendkívüli üzemeltetési helyzet leírása,
- a rendkívüli üzemeltetési helyzet hatása (ennek részeként biztonsági esemény esetén az érintett szolgáltatások, informatikai vagyonelemek és az érintett személyes adatok körének leírása, az érintett bizalmi szolgáltatási ügyfelek száma),

- a rendkívüli üzemeltetési helyzet várható időtartama,
- a rendkívüli üzemeltetési helyzet elhárítása és jövőbeli elkerülése érdekében tett és tervezett intézkedések, és
- a rendkívüli üzemeltetési helyzet megszűnése.

5.8 A szolgáltatás megszűnése

Szolgáltatónak a szolgáltatás megszüntetésekor teljesítenie kell a jogszabályokban megfogalmazott követelményeket.

A Szolgáltatás leállítása kapcsán a Szolgáltatónak az alábbi minimum intézkedéseket kell megtennie:

- A tervezett leállásról a szolgáltatási szabályzatban meghatározottak szerint értesítenie kell az Ügyfeleket és az Érintett feleket.
- Szolgáltatónak minden ésszerű erőfeszítést meg kell tennie annak érdekében, hogy egy erre alkalmas szolgáltató a nyilvántartásait és szolgáltatási kötelezettségeit legkésőbb a szolgáltatás leállításáig átvegye tőle.
- Szolgáltatónak kötelessége visszavonni a szolgáltatói tanúsítványokat, a hozzájuk tartozó magánkulcsokat pedig meg kell semmisítenie.
- Szolgáltatónak a szolgáltatás leállítása után közvetlenül egy teljes rendszermentést és archiválást kell végeznie;
- a rendszermentést és az archivált adatokat pedig át kell adnia a szolgáltatást átvevő szolgáltatónak vagy ennek hiányában a Bizalmi Felügyeletnek.

6 Műszaki biztonsági óvintézkedések

A szolgáltató köteles megfelelő intézkedéseket hozni az adathamisítás és az adatlopás ellen. Az időbélyegeket biztonságosan kell kibocsátani és a pontos időpontot kell belefoglalni. Az időpontot vissza kell tudni vezetni legalább egy UTC intézetre. Az időpontot a szabályzatokban és az időbélyegben megtalálható pontosság szerint kell szinkronizálni az UTC-vel, ügyelve arra, hogy ne csússzon ki ebből a pontosságból, ami nem lehet hosszabb 1 másodpercnél. Amennyiben a szolgáltató órája eltér ettől a pontosságtól, akkor azt szolgáltatónak észlelnie kell, s ilyen esetben időbélyeget nem bocsáthat ki. Az Időbélyegző Kiszolgáló óráját védeni kell minden olyan fenyegetettségtől, ami az időpont pontosságát észrevétlen módon lerontaná. Az időpontot, illetve annak szinkronizációját kezelni kell szökő másodperc esetén, s naplózni kell az eljárás pontos időpontját.
Az időbélyegeket olyan kulccsal kell aláírni, ami más célra nem kerül felhasználásra. A rendszernek vissza kell utasítania időbélyeg kiadását az időbélyegző kulcs érvényességét követően.
Amennyiben Szolgáltató minősített és nem minősített időbélyegeket egyaránt kibocsát, akkor a két szolgáltatást különböző elérési pontokon kell hozzáférhetővé tennie és eltérő Alany azonosítóval rendelkező tanúsítvánnyal hitelesítve adhatja csak ki azokat.
A minősített időbélyegeket olyan magánkulccsal kell aláírni, amely ellenőrzésére minősített tanúsítvány szolgál.
Szolgáltatónak biztosítani kell a minősített időbélyegző szolgáltatás folyamatosan rendelkezésre állását. Egy eseti szolgáltatáskiesés időtartama nem haladhatja meg a három órát.

6.1 Kulcspár generálás és telepítés

6.1.1. Kulcspár előállítása

Szolgáltatónak a kulcsokat védett módon kell generálni és a magánkulcsok bizalmasságáról gondoskodnia kell.

A szolgáltatói kulcsok generálására vonatkozóan az alábbiakat kell követni:

- A szolgáltatói kulcsok generálását - beleértve az időbélyegző kulcsokat is - és a nyilvános kulcs tanúsítását fizikailag védett környezetben kell megvalósítania legalább két bizalmi munkakört betöltő személy együttes részvételével, más személy jelenlétének kizárásával. E műveletre feljogosított munkatársak számát a minimumon kell tartani és a tevékenységnek a szabályzatokkal összhangban kell zajlani.
- A szolgáltatói kulcsok generálásánál - beleértve az időbélyegző kulcsokat is - csak olyan algoritmus és kulcshosszúság használható, amely megfelel az adott felhasználási célra vonatkozó szabványoknak, illetve a Nemzeti Média- és Hírközlési Hatóság engedélyezett algoritmusokra és minimális kulcsméretekre vonatkozó határozatának a tanúsítvány érvényességi ideje alatt.
- A szolgáltatói kulcsok generálására csak olyan kriptográfiai modulok alkalmazhatók, amelyek megfelelnek a szolgáltató szabályzataiban nyilvánosságra hozott műszaki és egyéb követelményeknek. A kulcsok nem importálhatók olyan eszközökbe, amelyek az alkalmazásra vonatkozó elvárásokat nem teljesítik.
- A ténylegesen alkalmazott algoritmusokat a Szolgáltatási szabályzatban fel kell tüntetni.
- Szolgáltatónak dokumentált eljárásokkal kell rendelkeznie a szolgáltatói kulcsok generálására, aminek legalább a következőket kell tartalmaznia:
    - Munkakörök, akik részt vesznek az eljárásban (akár belső, akár külső résztvevőről van szó);
    - A munkakörök által végrehajtandó feladatok az egyes fázisokban;
    - Felelősségek az eljárás során és azt követően;
    - Az eljárás során végrehajtandó adminisztrációs feladatok (amik bizonyítékul is szolgálnak a későbbiekben a megfelelésre).
- A szolgáltatónak az eljárás során egy olyan riportot kell előállítania, ami bizonyítja, hogy az megfelelt a szabályozásnak, és a kulcspár integritása és bizalmassága biztosított volt. A riportot alá kell írnia annak a bizalmi munkakört betöltő személynek, aki felelős a kulcsgenerálásért, és aki az eljárást követve biztosítja, hogy a riport hűen dokumentálja a végrehajtott eljárást.

A szolgáltató kulcsokat - beleértve az időbélyegző kulcsokat is - egy biztonságos kriptográfiai modulban kell generálni, ami megfelel 6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások fejezetben ismertetett elvárásoknak.
Amennyiben ugyanaz az időbélyegző kulcs több kriptográfiai modulban is alkalmazásra kerül, akkor ugyanazt a tanúsítványt kell hozzá kapcsolni. Egy időben azonban egy Időbélyegző Kiszolgálóban csak egy kulcs lehet aktív.

6.1.2. Magánkulcs eljuttatása Végfelhasználóhoz

Nem értelmezett.

6.1.3. A nyilvános kulcs eljuttatása a tanúsítványkibocsátóhoz

Nem értelmezett.

6.1.4. Az időbélyegző nyilvános kulcs közzététele

A szolgáltatónak a szolgáltatói nyilvános kulcsot - beleértve az időbélyeg kulcsot - a szolgáltatói tanúsítványai részeként Interneten elérhetővé kell tennie az érintett felek számára.

6.1.5. Kulcsméretek

A 6.1.1 fejezetben megfogalmazottak az irányadók.

6.1.6. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

Nem értelmezett.

6.1.7. A kulcshasználat célja

Az időbélyegző kulcsa kizárólag időbélyeg válaszok hitelesítésére alkalmazható.

6.2 Magánkulcs védelem és kriptográfiai modul előírások

Szolgáltatónak a magánkulcsát biztonságos módon kell tárolnia. Meg kell akadályoznia, hogy a szolgáltatói magánkulcshoz jogosulatlan személy hozzáférhessen, és a kulcsot arra jogosulatlan személy használhassa, lemásolhassa, törölhesse vagy módosíthassa.

A minősített szolgáltató az időbélyegző tanúsítványok előállításához, a magánkulcsokat csak fizikailag védett környezetben, az adott kulcsra meghatározott rendeltetési célra használhatja fel.

A hardveres kriptográfiai eszközök kezelése során a használatból kivont eszközökben tárolt aláíró vagy bélyegző magánkulcsokat olyan módon kell törölni, hogy azok visszaállítása ne legyen lehetséges.

6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások

A szolgáltatói magánkulcs - beleértve az archiváló rendszerben használt kulcsokat is - tárolásának és felhasználásának egy biztonságos kriptográfiai eszközön kell megvalósulni, amely:

- Legalább EAL4 tanúsítással rendelkezik az ISO/IEC 15408 vagy azzal ekvivalens IT biztonsági elvárásrendszer szerint; vagy
- Megfelel az ISO/IEC 19790 vagy a FIPS PUB 140-2 [12] elvárásainak 3. szinten.

Szolgáltatónak elkülönítve kell kezelni és működtetni

- a minősített szolgáltatás nyújtásához használt bizalmi szolgáltatást megvalósító termékeit az egyéb tevékenységeihez használt termékektől;
- a minősített szolgáltatások nyújtásához használt bizalmi szolgáltatást megvalósító termékeit a nem minősített szolgáltatásokhoz használt bizalmi szolgáltatást megvalósító termékektől.

Szolgáltatónak a bizalmi szolgáltatást megvalósító termékeit a szolgáltatási szabályzatban

meghatározott kockázatelemzések alapján biztonsági osztályokba kell sorolnia, és ezekről nyilvántartást vezetnie.

Szolgáltató egyéb tevékenységeihez használt termékek nem befolyásolhatják a bizalmi szolgáltatást megvalósító termék megbízható üzemeltetését.

Mielőtt a minősített szolgáltató a minősített szolgáltatás nyújtásához használt bizalmi szolgáltatást megvalósító termékeit a saját maga által végzett szolgáltatásnyújtáson kívüli célokra használja fel, meg kell bizonyosodnia arról, hogy a termék nem tartalmaz olyan adatot, amely bizalmi szolgáltatáshoz fűződik, valamint arról, hogy az ilyen adatot nem lehet visszaállítani. E vizsgálatot és a vizsgálat eredménye alapján végrehajtott intézkedést a minősített szolgáltatónak naplóznia kell.

6.2.2 Magánkulcs többszereplős (n-ből m) használata

Szolgáltató belső Biztonsági Szabályzatának részletes leírást kell tartalmaznia a többszereplős magánkulcskezelés módjáról. Amennyiben jelen Szolgáltatási Rend vagy a Szolgáltatási Szabályzat egy magánkulcs többszereplős kezelését írja elő, az adott művelet végzésére felhatalmazott bizalmi munkatársaknak ezen leírás szerint kell eljárniuk.

6.2.3. Magánkulcs letétbe helyezése

Szolgáltató az időbélyeg-szolgáltatás nyújtása során használt szolgáltatói aláíró magánkulcsokat nem helyezheti letétbe.

6.2.4. Magánkulcs mentése

Szolgáltatói magánkulcsairól - időbélyegző kulcs - Szolgáltatónak biztonsági másolatokat kell készítenie. A szolgáltatói magánkulcsok mentését (másolását), tárolását és helyreállítását Szolgáltatónak fizikailag védett környezetben, a többszereplős magánkulcskezelés szabályai szerint kell megvalósítania legalább két bizalmi munkakört betöltő személy együttes részvételével. E műveletre feljogosított munkatársak számát a minimumon kell tartani és a tevékenységnek a szabályzatokkal összhangban kell zajlani.

A szolgáltatói magánkulcs biztonsági mentéséből/mentéseiből legalább egy példányt a szolgáltatás nyújtásától eltérő helyszínen kell tárolni.

A szolgáltatói magánkulcs számára a kriptográfiai eszközön kívül is az eszköz által biztosított védelmi szintet kell biztosítani. A kulcs titkosítása során olyan algoritmust és kulcsméretet kell alkalmazni, ami annak teljes hátralévő idejében biztosítja a védelmet. A szolgáltatói magánkulcs nem üzemben lévő másolatait legalább a produktív kulccsal azonos szintű biztonsági eljárásokkal kell védeni.

6.2.5. Magánkulcs archiválása

Szolgáltató nem archiválhatja szolgáltatói magánkulcsait.

6.2.6. Magánkulcs bejuttatása kriptográfiai modulba, vagy onnan történő exportja

A szolgáltatói magánkulcsok kriptográfiai modulba juttatását Szolgáltatónak fizikailag védett

környezetben, a többszereplős magánkulcskezelés szabályai szerint kell megvalósítania legalább két bizalmi munkakört betöltő személy együttes részvételével.

6.2.7. Magánkulcs tárolása kriptográfiai modulban

Amennyiben a szolgáltatói magánkulcs egy dedikált kriptográfiai eszközön került tárolásra, akkor gondoskodni kell arról, hogy a kulcsok ne legyenek elérhetők az eszközön kívül.

A kriptográfiai eszköz esetében gondoskodni kell a hamisítás elleni védelemről a szállítás és a tárolás során is, és biztosítani kell a helyes működését.

6.2.8. A magánkulcs aktiválásának módja

A szolgáltatói magánkulcsok aktiválását Szolgáltatónak fizikailag védett környezetben, a többszereplős magánkulcskezelés szabályai szerint kell megvalósítania legalább két bizalmi munkakört betöltő személy együttes részvételével.

6.2.9. A magánkulcs deaktiválásának módja

Nincs előírás

6.2.10. A magánkulcs megsemmisítésének módja

A lejárt vagy használaton kívül helyezett szolgáltatói magánkulcsok minden (éles, mentett vagy archivált) példányát meg kell megsemmisíteni, olyan módon hogy az ne legyen visszaállítható, illetve használható.

Kriptográfiai eszköz megsemmisítése esetén gondoskodni kell a rajta tárolt magánkulcsok megsemmisítéséről (ez az előírás nem vonatkozik a kulcs összes példányára, csak az eszközön lévőre).

6.2.11. A kriptográfiai modulok értékelése

Lásd a 6.2.1 fejezetet.

6.3 A kulcspárkezelés további szempontjai

A Szolgáltató köteles a Kikötéseknek és a törvényi előírásoknak megfelelően használni és kezelni szolgáltatói kulcsait, különös tekintettel az alábbiakra:

- Szolgáltató saját szolgáltatói kulcsait nem használhatja a hozzájuk tartozó szolgáltatói tanúsítványok érvénytelensége esetén és a kulcspár használati idején túl (lásd 6.3.2).
- Az időbélyegzés szolgáltatás kapcsán, az Ügyfelek részére kibocsátott időbélyegek hitelesítésére használt kulcsok nem használhatók semmilyen más célra. A kulcsok csak fizikailag védett helyszínen használhatók. A Szolgáltatói magánkulcsnak kompatibilisnek kell lenni a tanúsítványok aláírására alkalmazott hash-lenyomat képző és aláíró eljárásokkal és kulcshosszakkal.

Az időbélyegző tanúsítványok érvényességi ideje nem haladhatja meg azt az időt, amely időpontig az alkalmazott kriptográfiai algoritmusok biztonságosan felhasználhatók.
Az időbélyegző tanúsítványokat egy a bizalmi felügyelet által nyilvántartásba vett Szolgáltatónak kell kibocsátania.
Az Időbélyegző Kiszolgáló nem bocsáthat ki időbélyegeket mielőtt a tanúsítványa betöltésre

került a kriptográfia egységbe, s a tanúsítvány teljes körű ellenőrzése megtörtént.

6.4 Aktiváló adat

Az aktiváló adattal kapcsolatos kérdéseket az alábbi fejezetek írják le.

A Szolgáltatói kulcspár telepítése és helyreállítása a kriptográfiai eszközön kizárólag bizalmi munkakörben foglalkoztatott munkatársak legalább kettős kontrollja alatt valósulhat meg.

6.4.1 Aktiváló adat generálás és telepítés

A szolgáltatói Aktiváló adat előállításának biztonságosan kell megvalósulni.

6.4.2 Aktiváló adat védelme

A szolgáltató kulcsának aktiválási adatát kizárólag a szolgáltató ismerheti meg.

6.5 Informatikai biztonsági előírások

Szolgáltatónak rendelkeznie kell az időbélyegzési tevékenység számára megfelelő minőségbiztosítási és információbiztonság menedzsment rendszerrel.

6.6 Életciklusra vonatkozó biztonsági előírások

6.6.1 Rendszerfejlesztési előírások

A biztonsági követelmények elemzését el kell végezni a - Szolgáltató által vagy az ő megbízásából végzett - rendszerfejlesztési projektek tervezési és követelmény meghatározási szakaszában, annak érdekében, hogy a biztonság be legyen építve az informatikai rendszerekbe.
Változáskezelési eljárásokat kell alkalmazni a Szolgáltatói szoftver új verzióinak kiadásai, a szoftvermódosítások és szoftverjavítások esetén, valamint a konfigurációváltozásokra, amelyek a Szolgáltató biztonsági szabályait érintik. Az eljárások között szerepelni kell a dokumentáció aktualizálásának is.
Szolgáltatónak biztosítania kell a minősített szolgáltatás nyújtásához a szabályozott változáskezelést és a megbízható üzemeltetést, továbbá az üzemeltetés elválasztását a fejlesztéstől.

6.6.2 Biztonságkezelési előírások

A Szolgáltatónak megbízható rendszereket és termékeket kell használnia, amelyek védettek változtatásokkal szemben, és biztosítják az általuk támogatott eljárások technikai biztonságát és megbízhatóságát.

- A Szolgáltatói rendszereket és információkat védeni kell a vírusok, a rosszindulatú és a nem engedélyezett szoftverektől.
- Eljárásokat kell megállapítani és végrehajtani az összes megbízható és adminisztratív szerepkörre, amelyek hatással vannak a szolgáltatások nyújtására.
- Szolgáltatónak eljárásokat kell meghatározni és alkalmazni biztosítandó, hogy:

    - a biztonsági javítások ésszerű időn belül (legfeljebb 6 hónapon belül) alkalmazásra kerülnek, miután azok megjelentek;
    - A biztonsági javítások nem alkalmazhatók, ha azok olyan plusz biztonsági réseket tartalmaznak vagy instabilitást okozhatnak, amelyek hátrányosabbak, mint a kínált javítás; és a nem alkalmazás okai dokumentálásra kerültek.

Szolgáltatónak megbízható rendszereket kell használni a számára szolgáltatott adatok ellenőrizhető formában történő tárolására, olyan módon, hogy:

- az adatok kizárólag annak a személynek a hozzájárulásával legyenek nyilvánosan kereshetők, akire az adatok vonatkoznak;
- kizárólag arra feljogosított személyek végezhessenek bejegyzéseket és változtatásokat a tárolt adatokon;
- ellenőrizhető legyen az adatok hitelessége.

6.6.3 Életciklusra vonatkozó biztonsági előírások

Szolgáltatónak figyelemmel kell követnie az erőforrások igénybevételét és előrejelzéseket kell készítenie a jövőbeni kapacitásszükségletek várható alakulásáról, annak érdekében, hogy elegendő teljesítmény és tárterület álljon rendelkezésre.

6.7 Hálózati biztonság

A Szolgáltatónak a következő hálózati biztonsági feltételeknek kell megfelelni:

- A szolgáltatói rendszereknek legalább biztonságos zónán belül kell elhelyezkednie, s a szolgáltatónak biztonsági eljárással kell szavatolnia e rendszerek valamint a nagy biztonságú zónával való kommunikáció biztonságát.
- A szolgáltatói rendszerek esetében a szolgáltatásnyújtáshoz nem használt felhasználói fiókokat, alkalmazásokat szolgáltatásokat, kapcsolatokat, protokollokat és portokat tiltani kell vagy el kell távolítani. A meghatározott szabályokat rendszeresen felül kell vizsgálni.
- A szolgáltató a biztonságos zónához és a nagy biztonságú zónához csak megbízható szerepkörrel rendelkező munkatársnak adhat hozzáférést.
- A szolgáltatónak kockázatértékelés alapján különböző hálózatokba vagy zónákba kell szegmentálnia a rendszereit, figyelembe véve a megbízható rendszerekkel és szolgáltatásokkal való funkcionális logikai és fizikai kapcsolatokat.
- A szolgáltatói rendszerek számára külön hálózatot kell biztosítani. Az információbiztonsági szabályzat érvényesítésére használt rendszereket más célra nem szabad használni. A produktív rendszereknek el kell különülni a fejlesztési, teszt és egyéb felhasználású rendszerektől.
- A különböző megbízható rendszerek közötti kommunikációnak megbízható csatornán kell folynia, ami logikailag elkülönül az egyéb kommunikációs csatornáktól, s biztosítja a végpontok megbízható azonosítását és a forgalmazott adatok bizalmasságát és sértetlenségét.
- Amennyiben a szolgáltatáshoz nagy rendelkezésre állású külső elérés szükséges, akkor a hálózati kapcsolatnak redundánsnak kell lennie, hogy biztosítsa a szolgáltatás elérését amennyiben valamelyik kapcsolat kiesik.
- Szolgáltatónak rendszeresen sebezhetőségi ellenőrzést kell végeznie a nyilvános és privát IP címein és rögzítenie kell annak bizonyítékait, hogy a vizsgálatot olyan

független, a megfelelő ismeretekkel, tapasztalattal és eszközökkel bíró személy vagy szervezet végezte, amely megbízható riportot eredményez. Az ellenőrzést negyedévente vagy szignifikáns hálózati változás esetén kell elvégezni.

- A szolgáltatói rendszeren rendszeresen betörési ellenőrzést kell végezni és rögzítenie kell annak bizonyítékait, hogy a vizsgálatot olyan független, a megfelelő ismeretekkel, tapasztalattal és eszközökkel bíró személy vagy szervezet végezte, amely megbízható riportot eredményez. Az ellenőrzést évente vagy szignifikáns infrastrukturális változás, alkalmazásmódosítás esetén kell elvégezni.

7 Időbélyeg profilok

7.1 Időbélyegző kérés profil

Az Időbélyegző Kiszolgálónak és az Időbélyeget feldolgozó alkalmazásoknak támogatni kell az ETF RFC 3161 2.4.1 fejezete szerinti időbélyeg kérelmet[4] (a támogatandó mezők a következők: reqPolicy, nonce, certReq) és azokat a lenyomatképző algoritmusokat, amelyek megfelelnek a Bizalmi Felügyelet engedélyezett algoritmusokra és minimális kulcsméretekre vonatkozó határozatának. Ennek megfelelően Szolgáltató az ügyfelektől kizárólag sha256 vagy sha512 algoritmussal képzett hash-lenyomatot tartalmazó időbélyeg kérést fogadhat el.

7.2 Időbélyegző és időbélyeg válasz profilok

A Szolgáltató által kiállított időbélyegnek meg kell felelni az ETSI 319 422 időbélyeg profiljának, s a következő mezőket tartalmaznia kell:

- Policy mező az időbélyegzés hitelesítési rendjének azonosítására (lásd 1.2.1 Hitelesítési Rendek)
- genTime mező
- accuracy mező (a genTime mezőben található időpont pontosságát meghatározva)

Az ordering mezőt nem tartalmazhatja az időbélyeg vagy csak “hamis” értékkel, s egyik kiterjesztés sem lehet kritikusként megjelölve.
Az időbélyegző kizárólag a szolgáltató aláírását tartalmazhatja. A SignedData SigningCertificate vagy SigningCertificateV2 mezőjének signerInfo attribútumának tartalmaznia kell az időbélyegző tanúsítvány azonosítóját (ESSCertID vagy ESSCertIDv2).[5]
Az Időbélyegző Kiszolgálónak és az Időbélyeget feldolgozó alkalmazásoknak támogatni kell az ETF RFC 3161 2.4.2 fejezete szerinti időbélyeg választ[6] (a támogatandó mezők a következők: accuracy, nonce) és azokat az aláírási algoritmusokat és kulcshosszakat, amelyek megfelelnek a Nemzeti Média- és Hírközlési Hatóság engedélyezett algoritmusokra és minimális kulcsméretekre vonatkozó határozatának.
Amennyiben a nonce mező jelen volt az időbélyeg kérésben, akkor a válasznak tartalmaznia kell ugyanazt az értékű nonce mezőt.
A minősített időbélyegzőnek a qcStements kiterjesztést is ajánlott tartalmaznia az IETF RFC 3739 szabvány szerinti formában, az esi4-qtstStatement-1 értékkel, nem kritikus

[4] Lásd https://www.ietf.org/rfc/rfc3161.txt
[5] IETF RFC 3161 IETF RFC 5816
[6] Lásd https://www.ietf.org/rfc/rfc3161.txt

kiterjesztésként megjelölve.

7.3 Időbélyegző tanúsítvány profil

Az időbélyegző tanúsítványnak az ETSI EN 319 412-3 szerinti követelményeket teljesítenie kell. Az Alany countryName attribútumának jeleznie kell, hogy az időbélyeg szolgáltató mely országban került bejegyzésre. Az organizationName mezőnek a szolgáltató teljes hivatalosan bejegyzett cégnevét kell tartalmaznia. A commonName mezőnek az Időbélyegző egyedi elnevezését kell tartalmaznia.
Az időbélyegző tanúsítványnak meg kell felelni a Nemzeti Média- és Hírközlési Hatóság engedélyezett algoritmusokra és minimális kulcsméretekre vonatkozó határozatának.

7.4 Időbélyegző transport protokoll profil

Az Időbélyegző Kiszolgálónak és az Időbélyeget feldolgozó alkalmazásoknak támogatni kell az időbélyegző transport protokollt HTTP és HTTPS protokollokon[7]. A HTTPS protokoll alkalmazása preferált.

8 A megfelelőség vizsgálata

A Szolgáltatónak tevékenységét összhangban kell végeznie

- a vonatkozó és hatályos Európai Uniós és hazai szabályozással,
- jelen Bizalmi Szolgáltatási rend követelményeivel, valamint
- a működési helye szerinti Bizalmi felügyelet Bizalmi szolgáltatások nyújtására vonatkozó nyilvántartásában szerepelnie kell.

A szolgáltató tevékenységét a Nemzeti Média és Hírközlési Hatóság felügyeli, évente minimum egyszer átfogó helyszíni ellenőrzést tart.
A Szolgáltatónak tevékenységét külső megfelelőségértékelő szervezettel értékeltetnie kell a vonatkozó szabványoknak megfelelően, mielőtt időbélyegzőket bocsát ki.
A Szolgáltató külső megfelelőségértékeléséhez végzett vizsgálat során az alábbiakat kell betartani:

- figyelembe kell venni Szolgáltató összes értékelendő bizalmi szolgáltatás sajátosságát;
- biztosítani kell, hogy a vizsgálat tárgyához tartozó minden szolgáltatói tevékenységet lefedjen a vizsgálat;
- a vizsgálatot vonatkozó szabványok, nyilvánosan hozzáférhető specifikációk és/vagy jogszabályi követelmények alapján kell végezni.

8.1. Az ellenőrzések körülményei és gyakorisága

A Szolgáltató köteles folyamatosan ellenőrizni jelen Bizalmi Szolgáltatási rendjében és Szolgáltatási szabályzataiban foglaltak betartását valamint szigorú ellenőrzés alatt kell tartania szolgáltatásai minőségét önellenőrzések végrehajtásával. E cél megvalósulása érdekében a

[7] Lásd az IETF RFC 7230 - 7235 és az IETF RFC 2818 szabványokat és az IETF RFC 3161 3.4 fejezetét.

Szolgáltatónak évente egyszer belső audit kell tartania.
Amíg a Szolgáltató minősített időbélyeg-szolgáltatást nyújt, legalább évente köteles a vonatkozó szabványoknak való megfelelőséget belső auditok és külső megfelelőségértékelés elvégzésével vizsgálni.

8.2 Az értékelő és szükséges képesítése

A belső auditokat olyan szakembernek kell végeznie, aki felsőfokú képesítéssel és megfelelő szakmai gyakorlattal rendelkezik szabályozási, informatikai rendszeraudit vagy bizalmi szolgáltatási területen.
A külső megfelelőségértékeléseket olyan természetes vagy jogi személynek, avagy természetes személyek csoportjának kell végeznie, aki vagy amely rendelkezik egy EU tagállam nemzeti akkreditációs szervezetétől megfelelő felhatalmazással, valamint:

- képes a 8 A megfelelőség vizsgálata fejezetben megadott szabványokra vonatkozó audit elvégzésére;
- megfelel a 8.3 Az auditor és az auditált entitás kapcsolata fejezetben megadott követelménynek;
- megfelelő jártassággal bír vagy bírnak a Publikus Kulcsú Infrastruktúra (PKI), az IT illetve IT biztonsági megoldások, technológiák és auditok terén;
- ETSI szabványok alapján végzett auditok esetén rendelkezik vagy rendelkeznek
    - az ETSI EN 319 403 szerinti akkreditációval, *vagy*
    - egy ezzel egyenértékű nemzeti szabvány szerinti akkreditációval, *vagy*
    - a Nemzeti Akkreditációs Hatóság által ISO 27001 szerint végrehajtott ISO 27006 szerinti akkreditációval;
- WebTrust audit végzése esetén rendelkezik vagy rendelkeznek WebTrust audit elvégzéséhez szükséges engedéllyel;
- tevékenységét vagy tevékenységüket jogszabályok vagy szakmai etikai kódex szabályozza;
- rendelkezik az auditor tevékenység végzéséből eredő mulasztások, hibák esetére szóló, legalább egymillió USD fedezetű biztosítással.

8.3 Az auditor és az auditált entitás kapcsolata

A Szolgáltató a belső megfelelőségértékeléseket a Független rendszervizsgáló szerepkörrel felruházott bizalmi alkalmazottai segítségével is elvégezheti.
A külső megfelelőségértékeléseket olyan értékelő végezheti, aki vagy amely a Szolgáltató tulajdonosi körétől, vezetőségétől, üzemeltetésétől független.

8.4. Az értékelés által lefedett területek

Szolgáltató belső megfelelőségértékelésének az alábbi területeket kell lefednie:

- szabályzatok hatályos jogszabályoknak és szabványoknak való megfelelése;
- az alkalmazott folyamatok szabályzatoknak való megfelelősége.

Külső megfelelőségértékelés esetén a megfelelőségértékelőnek az adott értékelési rendszer által meghatározott követelmények és kritériumok teljesülését kell értékelnie.

8.5. A hiányosságok kezelése

A külső megfelelőségértékelések eredményét egy értékelésjelentésben kell összefoglalni. A jelentésben – amennyiben vannak – rögzíteni kell a vizsgálat során feltárt eltéréseket és az elhárításukra kitűzött határidőket.

8.6. Az eredmények közzététele

A Szolgáltató nem köteles a belső megfelelőségértékelési jelentés publikálására, az abban foglaltakat bizalmas információként kezelheti.
A Szolgáltatónak az auditidőszakot követő három (3) hónapon belül nyilvánosságra kell hoznia a külső megfelelőségértékelési jelentést. A Szolgáltató nem köteles nyilvánosságra hozni az auditjelentés azon általános megállapításait, melyek nincsenek hatással az audit eredményére.

9. Egyéb üzleti és jogi tudnivalók

9.1. Díjak

A Szolgáltató nyilvános árlistán köteles elérhetővé tenni az Előfizetők részére a szolgáltatások kapcsán alkalmazott díjakat.

9.1.1 Időbélyeg-szolgáltatás díjai

A Szolgáltató az időbélyeg-szolgáltatás igénybevételéért a nyilvános árlista alapján számíthat fel díjat Előfizető részére, illetve attól Előfizetővel való előzetes egyeztetés alapján eltérhet.

9.1.2 Visszatérítési politika

Nincs megkötés.

9.2. Pénzügyi felelősség

A Szolgáltató a mindenkor hatályos polgári törvénykönyvben meghatározott szerződésszegésért való felelősség szabályai szerint, s a mindenkor hatályos bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló rendeletben meghatározott mértékig; s a szolgáltatási szabályzatában, általános szerződéses feltételeiben foglaltaknak megfelelően felel a szolgáltatásaival okozott károkért.
A szolgáltató korlátozhatja a felelősségvállalása értékét, az Ügyfeleket és Érintett feleket a weboldalán keresztül tájékoztatva.

9.2.1 Biztosítási fedezet

A Szolgáltató köteles megbízhatóság érdelében felelősségbiztosítással rendelkezni. A felelősségbiztosításnak ki kell terjedni a szolgáltató által nyújtott bizalmi szolgáltatásokkal összefüggésben okozott károkra és költségekre:

- a bizalmi szolgáltatási ügyfélnek a bizalmi szolgáltatási szerződés megszegésével

összefüggésben okozott károkra,
- a bizalmi szolgáltatási ügyfélnek és harmadik személynek szerződésen kívüli okozott károkra,
- az Eüt.-ben foglalt kötelezettségek nem teljesítése miatt a bizalmi felügyeletnél felmerült, az Eüt. szerinti költségekre, és
- az eIDAS Rendelet vonatkozó rendelkezései alapján a bizalmi felügyelet által felkért megfelelőségértékelő szervek eljárásának költségeire, ha azt a bizalmi felügyelet eljárási költségként érvényesíti.

A szolgáltatónak biztosítania kell, hogy az általa kötött biztosítási szerződés kifejezetten nevesítse, hogy a szerződés kiterjed a fentiekre.
A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként nem lehet alacsonyabb, mint 3 000 000 (hárommillió) forint.

9.2.2 Egyéb eszközök

A Szolgáltató a szolgáltatás megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében
- legalább huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával kell rendelkeznie VAGY
- pénzügyi intézménynél óvadékot kell alapítania legalább huszonötmillió forint értékben VAGY
- Egy legalább százmillió forint jegyzett tőkéjű, az Európai Gazdasági Térségben letelepedett vállalkozás készfizető kezességével kell rendelkeznie legalább huszonötmillió forintig terjedően.

9.2.3 Az Érintett felek számára elérhető biztosítások és garanciák

A szolgáltató tegye közzé, hogy az általa nyújtott garanciák és biztosítások mennyiben terjednek ki más felek által okozott károkra.

9.3. Bizalmas üzleti információk kezelése

A Szolgáltató köteles az információs önrendelkezési jogról és az információszabadságról szóló jogszabály rendelkezéseinek megfelelően tárolni és kezelni a birtokába jutott bizalmas adatokat.

9.3.1 A bizalmas információk köre

A Szolgáltatónak bizalmas információnak kell tekintenie minden az egyes Ügyfelekre vonatkozó adatot, amik nem szerepelnek a 9.3.2 fejezetben.

9.3.2 A bizalmas információk körén kívül eső adatok

A Szolgáltatónak nem kell bizalmas információnak tekintenie azon adatokat, amiket személyes jellegüktől megfosztott (pl. anonimizálással).
A nem bizalmas adatokat Szolgáltató nyilvánosságra hozhatja, megoszthatja partnereivel, illetve nyilvánosságra kerülésükért nem tartozik felelősséggel.

9.3.3 A bizalmas információk védelme

A Szolgáltató felelősséggel tartozik az általa kezelt bizalmas adatok védelméért. Ezeket az adatokat csak azon munkatársai és partnerei ismerhetik meg, amelyek munkájához ezen adatok ismerete szükséges. Más személyek hozzáférését ki kell zárni jogi úton és lehetőség szerint műszaki-biztonsági óvintézkedésekkel.
Minden, a bizalmas adathoz hozzáférő személyt szerződésben vagy titoktartási nyilatkozat aláírásával kell kötelezni a bizalmasság megőrzésére.
A Szolgáltatónak a Szolgáltatási szabályzatában tételesen meg kell határoznia, hogy mely esetekben és kik számára fedheti fel a bizalmas adatokat.
Például:

- kötelező információszolgáltatás hatóságok részére,
- információszolgáltatás polgári és büntető eljárás keretében,
- Ügyfelek, valamint az érintett személyek kérésére történő adatszolgáltatás.

9.4. Személyes adatok kezelése

A Szolgáltatónak az Eüt., valamint az Info tv. vonatkozó rendelkezései alapján kell kezelnie a személyes adatokat.
A Szolgáltatónak a bizalmi szolgáltatás nyújtás során azokat az adatokat kell kezelnie, amelyek a szolgáltatás nyújtásához technikailag elengedhetetlenek.

A Szolgáltató köteles a hatályos jogszabályoknak megfelelően az időbélyeg-szolgáltatás nyújtásával kapcsolatos elektronikus információkat és az ahhoz kapcsolódó személyes adatokat legalább az időbélyeg kibocsátásától számított 10 évig, illetőleg az időbélyeggel, illetve az időbélyegzett dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi, valamint ugyanezen határidőig olyan eszközt biztosítani, mellyel a kibocsátott időbélyeg válasz tartalma megállapítható.
A Szolgáltató köteles biztosítani, hogy bármely adat rendelkezésre bocsátása esetén ezen adatokhoz illetéktelen személyek ne férhessenek hozzá. A Szolgáltató adatkezelésére vonatkozó alapelveit „A személyes adatok bizalmas kezelésének alapelvei” című dokumentum tartalmazza, mely mindenkor hatályos változata elérhető a Szolgáltató honlapján.

9.4.1 Adatkezelési szabályok

A Szolgáltató birtokába jutott adatokat a Szolgáltatónak az adatok védelméről, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezéseinek megfelelően kell kezelnie.
A szolgáltató csak a szolgáltatás nyújtásához szükséges személyes adatokat igényelheti, az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló direktívának megfelelően.
A Szolgáltatónak rendelkeznie kell adatkezelési szabályzattal, amely részletes előírásokat tartalmaz a bizalmas és személyes információk kezelésére. Az Adatkezelési szabályzatot vagy annak kivonatát a Szolgáltató honlapján elérhetővé kell tenni.

9.4.2. Személyes adatok

A Szolgáltató csak olyan személyes adatokat kezel, amely az adatkezelés céljának megvalósuláshoz elengedhetetlen, a cél elérésre alkalmas, s melyek kezeléséről az érintett feleket tájékoztatja. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.
A Szolgáltatónak bizalmas adatként kell kezelnie minden személyes adatot, kivéve a 9.3.2-ben és 9.4.3-ban megadott személyes adatokat.

9.4.3. Személyes adatnak nem minősülő információk

Nem értelmezett.

9.4.4. Személyes adatok védelme

A Szolgáltató köteles biztonságosan tárolni és védeni az időbélyeg-szolgáltatással kapcsolatban megismert és megőrzött személyes adatokat. Az adatokat megfelelő intézkedésekkel védeni kell a jogosulatlan hozzáférés és a megváltoztatás ellen, különösen az Ügyfél és a szolgáltató egyes egységei között történő továbbítás során. Továbbá védeni kell őket, az adatvesztés, a károsodás és a nem engedélyezet feldolgozás ellen. Lásd még az 5.3.1, 5.5.1, 5.7.1, 5.7.4 fejezeteket.

9.4.5. Személyes adatok felhasználása

A Szolgáltató a személyes adatokat csak olyan módon és mértékben használhatja fel, amely az időbélyeg szolgáltatással kapcsolatos műveletekhez (pl. az időbélyeg-URL eljuttatása Előfizetőhöz) szükséges.

9.4.6. Adatkezelés

A Szolgáltató az információs önrendelkezési jogról és az információszabadságról szóló törvény adatkezelési szabályait köteles betartani. A Szolgáltató személyes adatokat az érintett előzetes hozzájárulása alapján kezelhet.
A Szolgáltató személyes adatot akkor is kezelhet, ha az előzetes hozzájárulás beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése a Szolgáltatóra vonatkozó jogi kötelezettség teljesítése céljából szükséges vagy Szolgáltató vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.
A Szolgáltató csak a jogszabályok által meghatározott esetekben adhatja ki az Ügyfélről tárolt személyes adatokat az Ügyfél értesítése nélkül.

9.4.7. Egyéb adatvédelmi követelmények

Szolgáltató az általa nyújtott bizalmi szolgáltatások felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, vagy nemzetbiztonsági érdekből - az érintett személyazonosságát igazoló, valamint egyeztetett adatok tekintetében - az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén díjmentesen adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét rögzíteni kell, az adatátadásról a Szolgáltató az érintett Ügyfelet nem

tájékoztathatja.

9.5 Szellemi tulajdonhoz fűződő jogok

A Szolgáltató által ügyfelei részére kibocsátott időbélyegző tulajdonosa az Előfizető, teljes jogú felhasználója pedig a Végfelhasználó. A Szolgáltató által ügyfelei részére kibocsátott időbélyeg-URL tulajdonosa a Szolgáltató, teljes jogú felhasználója pedig a Végfelhasználó.
A jelen Bizalmi Szolgáltatási rend és szolgáltató további szabályzatai és dokumentációi a NetLock kizárólagos tulajdonát képezi. Az Ügyfelek, Végfelhasználók és egyéb Érintett felek e dokumentumokat csak jelen előírásoknak megfelelően jogosultak felhasználni, minden egyéb (pl. kereskedelmi) célú felhasználás szigorúan tilos. A nyilvános dokumentumok szabadon terjeszthetők, de csak változatlan formában, teljes terjedelemben és az eredet feltüntetésével.
A Bizalmi Szolgáltatási rendben, szolgáltató további szabályzataiban és dokumentációiban található védett nevek felett a jogtulajdonosuk rendelkezik. Az itt hivatkozott művek (szabványok, jogi források) szerzői joga a jog tulajdonosáé. A Szolgáltató működése során nem sértheti meg harmadik személyek szellemi tulajdonjogait.
A szolgáltatási tevékenység során alkalmazott szoftver és hardver komponensek a Szolgáltató tulajdonát képezik, vagy azokat jogszerűen használja.

9.6 Felelősség és garanciák

A Szolgáltató felelős jelen Bizalmi Szolgáltatási Rend és a Szolgáltatási szabályzata előírásainak betartásáért, abban az esetben is, ha egyes tevékenységeit kiszervezi.

9.6.1 A Hitelesítő Egység felelőssége

Nem értelmezett.

9.6.2 A Regisztrációs Egység felelőssége

A Regisztrációs Egység felelőssége:

- az Igénylők (személy-) azonosságának megállapítása, a szolgáltató rendelkezésére bocsátott adatok ellenőrzése;
- nem természetes személy előfizető esetén az Előfizető szervezeti azonosságának, a szervezet nevében eljáró személy személyazonosságának és képviseleti jogosultságának megállapítása, ellenőrzése;
- a szolgáltatási szerződésbe kerülő adatok valódiságának garantálása;
- a szolgáltatási szerződés megkötését megelőzően Ügyfél tájékoztatása a Bizalmi Szolgáltatási Rend és a Szolgáltatási Szabályzat tartalmáról és elérhetőségéről, a szolgáltatás igénybevételének feltételeiről;
- az időbélyeg URL-ek előállítása és Előfizetőnek történő továbbítása;
- általános kötelezettségeinek maradéktalan betartása.

9.6.3 Ügyfelek felelőssége és kötelezettségei

Az Ügyfél további kötelezettségeit és felelősségét az Általános szerződési feltételek, valamint a Szolgáltatási szerződés határozzák meg.

Ügyfél köteles:

- a Szolgáltatóval szolgáltatási szerződést kötni, vagy az általános szerződési feltételekkel megegyező megállapodást kötni;
- a szolgáltatási szerződés megkötéséhez valós adatokat megadni, valamint haladéktalanul tájékoztatni a Szolgáltatót ezen adatok változásáról;
- haladéktalanul tájékoztatni a Szolgáltatót a bizalmi szolgáltatással vagy az időbélyeggel kapcsolatban észlelt, a külön jogszabályban, szolgáltatási szerződésben illetve szolgáltatási szabályzatban meghatározott rendellenességről vagy más, a bizalmi szolgáltatást érintő eseményről, így különösen arról, ha a szolgáltatás használatához szükséges, a Szolgáltató által biztosított időbélyeg-URL-t jogosulatlan személy használhatta;
- haladéktalanul tájékoztatni a Szolgáltatót a bizalmi szolgáltatással kapcsolatos jogvita megindulásáról.

A tesztelési célra kibocsátott időbélyegeket Végfelhasználó nem használhatja valódi kötelezettségvállalásra alkalmas dokumentum vagy adat időbélyegzésére.

9.6.4 Érintett felek felelőssége

Az Érintett felek a bizalmi listán ellenőrizhetik az Időbélyegző Kiszolgáló és az időbélyeg minősített voltát. Amennyiben az Időbélyegző Kiszolgáló nyilvános kulcsa a bizalmi listán feltüntetésre kerül minősített időbélyegző szolgáltatást reprezentálva, akkor az Időbélyegző Kiszolgáló által kibocsátott időbélyegzők minősítettnek tekintendők. Az esi4-qtstStatement-1 qcStatement alkalmazásával a Szolgáltató azt jelzi, hogy az időbélyegzőt minősítettként bocsátotta ki.

9.6.5 Egyéb résztvevők felelőssége

Amennyiben a szervezet képviselője nem személyesen jár el az időbélyeg-szolgáltatás igénylése során, úgy a képviselt szervezet felelősséggel tartozik az általa kiadott igazolásokért, különös tekintettel azon igazolásokra, amelyben azt igazolja, hogy az Igénylő jogosult a Szervezet nevében a szolgáltatás igénylésére.

9.7 Szavatosság kizárása

A Szolgáltató kizárja a szavatosságot, amennyiben:

- az Érintett fél nem körültekintően jár el az időbélyegek felhasználása vagy ellenőrzése során, azaz nem a jelen Bizalmi Szolgáltatási rend, a Szolgáltatási szabályzat vagy a hatályos jogszabályok szerint jár el;
- az Érintett felek vagy mások által kibocsátott szabályzatok nem felelnek meg a jelen Bizalmi Szolgáltatási rendnek vagy a Szolgáltatási szabályzatnak;
- a Szolgáltató az Internet, vagy egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- a károkozás a Felügyeleti szerv által jóváhagyott kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8 Felelősség korlátozása

A Szolgáltató kártérítési felelősségét a Bizalmi Szolgáltatási Szabályzatának 9.2 pontja szerint korlátozhatja.

9.9 Kártérítés, kártalanítás

A Szolgáltató felelős minden olyan kárért, amelyet szándékosan vagy gondatlanul bármely természetes vagy jogi személynek okozott a vállalt kötelezettségének megszegéséből eredően.
A nem minősített Szolgáltató szándékosságát vagy gondatlanságát annak a természetes vagy jogi személynek kell bizonyítania, aki/amely állítása szerint a kár megtérítését követeli.
A minősített bizalmi szolgáltató szándékosságát vagy gondatlanságát vélelmezni kell, kivéve, ha a minősített bizalmi szolgáltató bizonyítja, hogy a kár a szándékos vagy gondatlan közrehatása nélkül következett be.
Amennyiben a Szolgáltató előzetesen megfelelően tájékoztatja ügyfeleit az általuk nyújtott szolgáltatások igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások harmadik felek számára felismerhetők, a Szolgáltató nem felelős a szolgáltatások igénybevételéből eredő, a jelzett korlátozásokat meghaladó károkért.
Minden egyéb esetben a mindenkori hatályos polgári törvénykönyv vonatkozó rendelkezései az irányadóak.

9.10 A Szolgáltatási rend hatálya

A Bizalmi Szolgáltatási rend aktuális verziójának időbeli hatálya a fedlapon jelzett hatálybalépés dátumával kezdődik és visszavonásig hatályos.
A Bizalmi Szolgáltatási rend személyi hatálya a Szolgáltatóra, annak a Szolgáltatásokban közreműködő munkatársaira, valamint az Ügyfelekre terjed ki.
A Bizalmi Szolgáltatási rend tárgyi hatálya kiterjed a Szolgáltató által nyújtott Szolgáltatásra, illetve az ennek keretében kibocsájtott időbélyegekre, valamint Szolgáltatónak a fenti Szolgáltatásokkal kapcsolatban álló összes objektumára és tárgyi eszközére.

9.10.1 Érvényesség

A Bizalmi Szolgáltatási rend adott verziója hatályba lépésének napja a dokumentum fedlapján kerül meghatározásra.

9.10.2 Megszűnés

A Bizalmi Szolgáltatási rend érvényessége megszűnik egy újabb Bizalmi Szolgáltatási Rend verzió hatályba lépésével vagy a szolgáltatási tevékenység beszüntetésekor.

9.10.3 A megszűnés következményei

A Bizalmi Szolgáltatási rend visszavonása esetén a Szolgáltató honlapján teszi közzé a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket.
A Szolgáltató vállalja, hogy a Bizalmi Szolgáltatási rend visszavonása esetén is érvényben

maradnak a mindenkor hatályos vonatkozó jogszabályokban meghatározott bizalmas adatok védelmére vonatkozó előírások.

9.11 Egyedi értesítések és a résztvevők közti kommunikáció

A Szolgáltató az Ügyfelekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát, telefonos ügyfélszolgálatot működtet.

9.12 A módosítás

A Szolgáltató a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén megváltoztatja a Bizalmi Szolgáltatási rendjét, a vonatkozó szabályzatait. Rendkívüli esetben a változások azonnali hatállyal is életbe léptethetők.
Szolgáltató köteles a bizalmi felügyelet számára bejelenteni, ha a bejelentések alapján nyilvántartásba vett adatokhoz képest működésében vagy a bizalmi szolgáltatás nyújtásában változás történik.

9.12.1 A módosítási eljárás

Szolgáltató a szabályzatváltoztatási igényeket gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz, s a változtatásokat életbe lépteti. A változtatásokat gyűjtve az egység belső, nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. Szolgáltató a változásokat kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.
A Szolgáltató jóváhagyás előtt megvizsgálja a Bizalmi Szolgáltatási Rendet és a szolgáltatási szabályzatokat, hogy tartalmilag és formailag megfelel-e hatályos jogszabályi követelményeknek. A Bizalmi Szolgáltatási rend és a szabályzatok jóváhagyására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik.
A módosított Bizalmi Szolgáltatási rend és szabályzatok változatai mindig új verziószámmal kerülnek nyilvánosságra. A Bizalmi Szolgáltatási rend és a szabályzatok valamint a vonatkozó jogszabályoknak és szabványoknak való megfelelés vizsgálata legalább évente történik. A szabályzatok rendkívüli felülvizsgálatára és módosítására a jogszabályi változások esetén kerül sor. A Bizalmi Szolgáltatási rend és a szabályzatok felülvizsgálatát a Szolgáltató a működése során szerzett gyakorlati tapasztalatok alapján is elvégzi.

9.12.2 Az értesítések módja és határideje

A minősített bizalmi szolgáltatást nyújtó szolgáltató a változás bekövetkeztét legalább 30 nappal megelőzően értesíti a bizalmi felügyeletet a nyilvántartásba vett adatokhoz képest működésében vagy a bizalmi szolgáltatás nyújtásában bekövetkező, tervezett változásokról.

9.12.3 A dokumentumazonosító változása

Szolgáltató a Bizalmi Szolgáltatási rend változtatása esetén új verziószámot kell adjon a dokumentumnak, így az az OID változását is eredményezi egyben, vagyis a két eltérő tartalmú dokumentumnak nem lehet azonos OID azonosítója.
A módosított szabályzat csak az újonnan kibocsátásra kerülő időbélyegekre vonatkozhat (de a már kibocsátottakra nem). Szolgáltató az új szabályzatokat előző verziótól eltérő Internet címen tegye közzé.

9.13 Vitás kérdések rendezése

A Szolgáltató köteles biztosítani a panaszok bejelentésének elérhetőségét, a panaszok kezelését, valamint köteles tájékoztatni a szolgáltatással összefüggő jogviták peres és peren kívüli kezdeményezésének lehetőségéről, annak feltételeiről, a békéltető testülethez való fordulás jogalapjáról, az eljárásra jogosult hatóságok és békéltető testület vagy más vitarendező szervezetek megnevezéséről, elérhetőségeiről.

9.14 Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar és európai uniós jogszabályoknak megfelelően végzi. A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

9.15 A hatályos jogszabályoknak való megfelelés

Szolgáltatónak bizalmi szolgáltatásait a mindenkor hatályos európai uniós és magyarországi szabályozásnak megfelelően kell nyújtania. A vonatkozó jogszabályokat és az azoknak való megfelelés módját Szolgáltató szolgáltatási szabályzataiban adja meg.

A jelen Szolgáltatási Rend hatálybalépésekor hatályos jogszabályok és szabványok:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről
- 26/2016. (VI. 30.) BM rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 421
- ETSI EN 319 422
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 2013. évi V. törvény a Polgári Törvénykönyvről
- A digitális archiválás szabályairól szóló 114/2007 (XII. 29.) GKM rendelet

9.16.1 Teljességi záradék

Nincs megkötés.

9.16.2 Átruházás

A jelen Bizalmi Szolgáltatási rendnek megfelelően működő szolgáltató csak a Szolgáltató előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

9.16.3 Részleges érvénytelenség

A jelen Bizalmi Szolgáltatási rend egyes rendelkezéseinek bármilyen okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4 Igényérvényesítés

A Szolgáltató kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt az Ügyfelektől az általuk okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben a Szolgáltató egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben, vagy a Bizalmi Szolgáltatási rend más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5 Vis maior

A Szolgáltató nem felelős a Bizalmi Szolgáltatási rendben és a Szolgáltatási szabályzatban megfogalmazott követelmények hibás vagy késedelmes teljesítéséért, ha a hiba vagy késedelem oka a Szolgáltató ellenőrzési körén kívül eső, előre nem látható körülmény volt.

9.17 Egyéb rendelkezések

A vezető munkatársaknak függetlennek kell lenni minden olyan üzleti, pénzügyi és más befolyástól, ami hátrányosan hathat a szolgáltatásokba vetett bizalomra.